

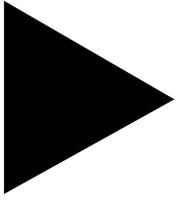
ExtremeWare Enterprise Manager™ Installation and User Guide

Version 2.0

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
<http://www.extremenetworks.com>

Published: November 1999
Part number: 100008-00 Rev A

©1999 Extreme Networks, Inc. All rights reserved. Extreme Networks and BlackDiamond are registered trademarks of Extreme Networks, Inc. in certain jurisdictions. ExtremeWare, ExtremeWare Vista, ExtremeWare Enterprise Manager, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS, the BlackDiamond logo and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodriven logo is a service mark of Extreme Networks, which may be registered or pending registration in certain jurisdictions. All other registered trademarks, trademarks and service marks are property of their respective owners. Specifications are subject to change without notice.



Contents

PREFACE

Introduction	xvii
Terminology	xviii
Conventions	xviii
Related Publications	xviii

1 EXTREMEWARE ENTERPRISE MANAGER OVERVIEW

Introduction	1-1
Summary of Features	1-2
ExtremeView Configuration and Status Monitoring	1-2
Enterprise-wide VLAN Management	1-3
Support for Summit Virtual Chassis Stacks	1-3
Policy-based Quality of Service	1-4
Simple Inventory Management	1-4
Real-Time Statistics	1-5
The MAC/IP Address Finder	1-5
Security Management	1-5
ExtremeWare Enterprise Manager Components	1-6
Extreme Networks Switch Management	1-7
Hardware and Software Requirements	1-8
Extreme Networks Device Requirements	1-8
Third-Party Device Requirements	1-8
Server Requirements	1-9
Client Requirements	1-10

2 INSTALLING THE EXTREMEWARE ENTERPRISE MANAGER

- Installation Overview 2-1
- Installing on a Windows NT System 2-2
 - Installing the Enterprise Manager Server 2-2
 - Updating an Evaluation Version to a Licensed Version 2-5
 - Uninstalling the Enterprise Manager Server 2-6
- Installing on a SPARC Solaris System 2-6
 - Installing the Enterprise Manager Server 2-7
 - Updating an Evaluation Version to a Licensed Version 2-12
 - Uninstalling the Enterprise Manager Server 2-13
- Installing the Enterprise Manager Client 2-14
 - Downloading the Client Applet in Internet Explorer 2-14
 - Uninstalling the Client Applet 2-16

3 STARTING THE EXTREMEWARE ENTERPRISE MANAGER

- Running the Enterprise Manager Under Windows 3-1
 - Starting or Restarting the Enterprise Manager Server 3-2
 - Shutting Down the Enterprise Manager Server Components 3-2
 - Restarting the Enterprise Manager Server Components as Services 3-3
- Running the Enterprise Manager Under Solaris 3-4
 - Starting or Restarting the Enterprise Manager Server 3-4
 - Shutting Down the Enterprise Manager Server Components 3-4
- Launching the ExtremeWare Enterprise Manager Client 3-5
- Navigating The Enterprise Manager Functions 3-8
 - The Component Tree 3-11
 - The Status/Detail Information Panel 3-11
 - Moving the Component Tree Boundary 3-13
 - Resizing and Sorting Columns 3-13
 - Applet function buttons 3-13

4 ADMINISTERING THE EXTREMEWARE ENTERPRISE MANAGER

- Overview of User Administration 4-1
 - Enterprise Manager Access 4-1
 - ExtremeWare Access 4-2
 - The RADIUS Server 4-2

Starting the Enterprise Manager Client for the First Time	4-3
Changing the Admin Password	4-4
Adding or Modifying User Accounts	4-6
Deleting Users	4-7
Changing Your Own User Password	4-8
RADIUS Administration	4-9

5 USING THE INVENTORY MANAGER

Overview of the Enterprise Manager Device Inventory	5-1
Device Groups	5-2
Port Groups	5-2
Gathering Device Status Information	5-2
Displaying the Network Device Inventory	5-3
Viewing Device Status Information	5-5
Discovering Network Devices	5-8
Adding Devices, Device Groups and Port Groups	5-13
Adding a Device	5-13
Creating a Device Group	5-15
Creating a Port Group	5-17
Modifying Devices, Device Groups and Port Groups	5-18
Modifying a Device	5-18
Modifying a Device Group	5-19
Modifying a Port Group	5-21
Deleting Devices, Device Groups, and Port Groups from the Database	5-22
Deleting a Device	5-22
Deleting a Device Group	5-24
Deleting a Port Group	5-24
Updating Device Information	5-25

6 USING EXTREMEVIEW

Overview of the ExtremeView Application	6-1
Viewing Switch Status Information	6-3
Viewing Switch Configuration Information	6-5
Viewing Switch Statistics	6-8
Using Telnet with Extreme Switches	6-9
Running ExtremeWare Command Macros	6-11
Running an Interactive Telnet Session on an Individual Switch	6-13

Copy/Paste from an Interactive Telnet Session	6-14
Macro Recording and Playback from an Interactive Telnet Session	6-15
Using Telnet with Cisco Devices	6-15

7 USING THE VLAN MANAGER

Overview of Virtual LANs	7-1
Displaying VLANs	7-2
Adding a VLAN	7-6
Deleting a VLAN	7-9
Modifying a VLAN	7-10
Adding and Deleting Protocol Filters	7-12

8 USING THE POLICY SYSTEM

Overview of The Policy System	8-1
Policy Types	8-2
Basic Policy Definition	8-5
Policy Objects	8-7
Policy Implementation Types	8-8
Policy Scoping	8-8
Policy Auto Configuration	8-8
Third-Party Device Support	8-9
Cisco Device Support	8-9
Cisco Port Mappings	8-10
Limitations on Cisco Device Support	8-10
Xedia Device Support	8-11
Limitations on Xedia Device Support	8-11
Using The Policy System	8-13
Creating a New Network Policy	8-15
Using the Create Policy Wizard	8-15
Creating a Policy from the New Menu	8-20
Viewing and Modifying Network Policies	8-21
The Definition Tab	8-23
VLAN Policy Definition Tab	8-23
Application Server Policy Definition Tab	8-24
Client/Server Policy Definition Tab	8-27
Source Port Policy Definition Tab	8-30

Custom Policy Definition Tab	8-32
The Status Tab	8-34
The Scope Tab	8-35
The Overlaps Tab	8-37
The Precedence Tab	8-38
The QoS Results Tab	8-41
Viewing and Modifying Network QoS Treatments	8-42
Adding or Modifying Local Users	8-44
Adding or Modifying User Groups	8-47
Adding or Modifying End Stations	8-48
adding or Modifying End Station Groups	8-50
Displaying Managed Device Status	8-52
Cisco Device Policy Setup	8-53
Configuring QoS Policies	8-55
System Status	8-56
Current State	8-56
Importing Data from NT Domains or Solaris NIS	8-57
Displaying the Event Log	8-58

9 MANAGING VIRTUAL CHASSIS STACKS

Overview of Virtual Chassis Stacks	9-1
Identifying Virtual Chassis Stack Topologies	9-2
Displaying the Virtual Chassis Stack Topology	9-3
Displaying A Virtual Chassis Stack	9-5
Displaying A VC Stack Component	9-6
Displaying Orphan VCs	9-7
Displaying Orphan Summit Switches	9-8
Creating a Virtual Chassis Stack	9-10
Deleting a Virtual Chassis Stack	9-11
Editing a Virtual Chassis Stack	9-12
Configuring Virtual Chassis Stack Ports	9-13
Identifying the Virtual Chassis Stack Topology	9-15

10 REAL TIME STATISTICS

- Overview 10-1
- Displaying Multiport Statistics 10-3
- Displaying Statistics For a Single Port 10-7
- Changing the Display Mode 10-9
- Setting Graph Preferences 10-11

11 USING THE IP/MAC ADDRESS FINDER

- Overview of the IP/MAC Finder Applet 11-1
- Tasks List Summary Window 11-2
- Creating a Search Task 11-4
- Detailed Task View 11-5

A HP OPENVIEW INTEGRATION

- Integration Overview A-1
- Integrating with HP OpenView under Windows NT A-2
 - Installing the HP OpenView Integration Components A-2
 - Uninstalling the Integration Components A-4
- Integrating with HP OpenView under Solaris A-4
 - Installing the HP OpenView Integration Components A-4
 - Uninstalling the Integration Components A-9
- Launching the Client from HP OpenView A-9
 - Launching the Client from the HP OpenView Tools Menu A-9
 - Launching ExtremeWare Vista from the HP OpenView Map A-11

B DYNAMIC LINK CONTEXT SYSTEM (DLCS)

- Overview B-1
- Using DLCS in the Policy System B-2
- DLCS Properties B-2
- Enabling DLCS on an Extreme Switch B-2
- DLCS Limitations B-3
 - ISQ Improvements B-4

C DATABASE UTILITIES

Overview C-1

The Validation Utility C-2

Using the DBVALID Command-line Utility C-2

Database Connection Parameters C-3

The Backup Utility C-3

The DBBACKUP Command-line Utility C-3

Database Connection Parameters C-4

Installing a Backup Database C-5

D EXTREMEWARE ENTERPRISE MANAGER PROPERTIES FILES

The extreme.properties File D-1

The ciscoipports.properties File D-2

E TROUBLESHOOTING

ExtremeWare Enterprise Manager Server Issues E-1

Installation E-1

SNMP E-2

VLANs E-3

ExtremeWare Enterprise Manager Client E-4

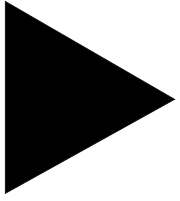
Client Initialization E-4

VLAN Manager E-5

Inventory Manager E-5

Policy System client E-6

INDEX



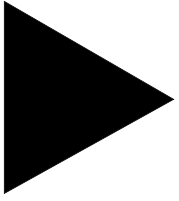
Figures

1-1	ExtremeWare Enterprise Manager software architecture	1-7
2-1	ExtremeWare Enterprise Manager Start-up page	2-15
2-2	Security warning prior to downloading the signed client applet	2-16
3-1	ExtremeWare Enterprise Manager Start-up page	3-6
3-2	ExtremeWare Enterprise Manager Login page	3-7
3-3	The About ExtremeWare Enterprise Manager page	3-9
3-4	VLAN Manager applet running in a browser window	3-10
3-5	Inventory Manager applet	3-12
3-6	Pop-up dialog box for adding a VLAN in the VLAN Manager	3-14
4-1	User Administration window	4-4
4-2	Edit User window	4-5
4-3	New User and Edit User windows	4-6
4-4	Change Password window	4-8
4-5	Radius Administration page	4-10
5-1	The Inventory Manager applet, main page	5-4
5-2	Inventory Manager device group summary status	5-6
5-3	Inventory Manager device status information	5-7
5-4	Inventory Manager information for a Cisco device	5-8
5-5	Inventory Manager Device Discovery set up window	5-9
5-6	Results of a discovery, with details visible	5-11
5-7	Setting default device options for discovered devices	5-12
5-8	Message window showing Add device progress	5-13
5-9	Add Device window in the Inventory Manager	5-14
5-10	Add Device Group window in the Inventory Manager	5-16

5-11	Add Port Group window in the Inventory Manager	5-17
5-12	Devices tab of the Modify Devices, Device Groups, and Port Groups window.	5-19
5-13	Device Groups tab of the Modify Devices, Device Groups, and Port Groups window.	5-20
5-14	Port Groups tab of the Modify Devices, Device Groups, and Port Groups window.	5-21
5-15	Devices tab of the Delete Devices and Device Groups window.	5-23
5-16	Device Groups tab of the Delete Devices, Device Groups, and Port Groups window.	5-24
5-17	Port Groups tab of the Delete Devices, Device Groups, and Port Groups window.	5-25
5-18	Synchronize Devices dialog	5-26
6-1	The ExtremeView applet, main page	6-2
6-2	The ExtremeView applet, Status summary	6-3
6-3	The ExtremeView applet, switch status	6-4
6-4	The ExtremeView applet, port status	6-5
6-5	The ExtremeView applet, Configuration summary	6-6
6-6	The ExtremeView applet, Configuration details	6-7
6-7	The ExtremeView applet, Statistics summary	6-8
6-8	The ExtremeView applet, Statistics details	6-9
6-9	The ExtremeView applet, Telnet interface	6-10
6-10	The ExtremeView applet, record and play buffer	6-11
6-11	An open Telnet session for a switch in the ExtremeView applet	6-13
6-12	An open Telnet session for a switch in the ExtremeView applet	6-14
6-13	An open Telnet session for Cisco device in ExtremeView	6-16
7-1	VLAN Manager applet, topology shown by VLAN	7-3
7-2	VLAN topology shown by switch	7-4
7-3	VLAN member ports on a selected switch	7-5
7-4	Switch member ports for a selected VLAN	7-6
7-5	Add VLAN dialog, Properties and Ports page	7-7
7-6	Add VLAN dialog, IP Forwarding page	7-8
7-7	The Delete VLAN page	7-9
7-8	The Modify VLAN dialog, Properties and Ports page	7-10
7-9	The Modify VLAN dialog, IP Forwarding page	7-12
7-10	Protocol Panel dialog box, View/Delete page	7-13

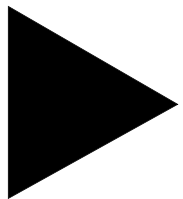
7-11	Protocol Panel dialog box, Add Protocol page	7-14
8-1	Application Server Policy	8-2
8-2	Client/Server Policy	8-3
8-3	Source Port Policy	8-4
8-4	VLAN Policy	8-4
8-5	Basic Policy Definition	8-6
8-6	The Policy System main view	8-13
8-7	Using the policy object selector to specify policy components	8-16
8-8	Pop-up selection box for Policy type	8-20
8-9	Create: Network QoS Policy page for a VLAN policy	8-21
8-10	Network QoS Policy view for a VLAN policy, Definition tab	8-22
8-11	Network QoS Policy view for an Application server policy, Definition tab	8-25
8-12	Translation of a Client/Server policy definition into traffic flows	8-27
8-13	Network QoS Policy view for a Client/Server policy, Definition tab	8-28
8-14	Network QoS Policy view for a Source Port policy, Definition tab	8-30
8-15	Network QoS Policy view for a Custom policy, Definition tab	8-32
8-16	Network QoS Policy view for a VLAN policy, Status tab	8-34
8-17	Network QoS Policy view for a VLAN policy, Scope tab	8-35
8-18	Network QoS Policy view for a VLAN policy, Overlaps tab	8-37
8-19	Network QoS Policy view for a VLAN policy, Precedence tab	8-39
8-20	Edit: Select Policies pop-up window	8-40
8-21	Network QoS Policy view for a VLAN policy, QoS Results tab	8-41
8-22	Network QoS Treatment view	8-43
8-23	The Network User View	8-45
8-24	The Local Group – Users view	8-47
8-25	The End Station view.	8-49
8-26	The End Station Group view.	8-51
8-27	The Managed Devices View	8-52
8-28	Setting Cisco Device Policy	8-53
8-29	The Policy System Configuration view.	8-55

8-30	The Import Data view	8-58
8-31	The Event Log	8-59
9-1	Virtual Chassis Stack Manager display of known Virtual Chassis stacks	9-4
9-2	Details of an individual Virtual Chassis Stack	9-6
9-3	Detail view of a Virtual Chassis component of a VC stack	9-7
9-4	Orphan Virtual Chassis Connections	9-8
9-5	Orphan switches Virtual Chassis connections	9-9
9-6	Creating a VC stack	9-10
9-7	Delete Virtual Chassis Stack	9-11
9-8	Editing a VC stack	9-12
9-9	Configure ports in a VC Stack	9-14
9-10	Identify Virtual Stack	9-16
10-1	Real Time Statistics main page	10-4
10-2	Bar chart showing device port statistics	10-5
10-3	Warning displayed when Enterprise Manager cannot retrieve data	10-6
10-4	Utilization data over time for an individual port on a device.	10-8
10-5	Individual errors in a single-port chart	10-9
10-6	Setting 3D graph preferences	10-11
10-7	Setting graph color preferences	10-12
10-8	Setting data color preferences	10-13
10-9	Setting other graph preferences	10-13
11-1	IP/MAC Address Finder main page	11-2
11-2	Tasks List summary	11-3
11-3	Find addresses window	11-4
11-4	Search in progress	11-6
11-5	Address search results in the Detailed Task View	11-7
A-1	The Tools menu in HP OpenView Network Node Manager	A-10
A-2	ExtremeWare Enterprise Manager icon on the HP OpenView toolbar	A-11
A-3	Pop-up menu for a selected Summit device	A-12



Tables

1	Text Conventions	xviii
5-1	Inventory Manager Device Status Indicators	5-6
6-1	ExtremeView Switch Status Indicators	6-4
6-2	ExtremeView Macro Variables	6-12
8-1	Default QoS Treatments	8-43
C-1	dbvalid Command Switches	C-2
C-2	Database Connection Parameters for dbvalid Utility	C-3
C-3	dbbackup Command Switches	C-4
C-4	Database Connection Parameters for dbbackup Utility	C-4



Preface

This Preface provides an overview of the ExtremeWare Enterprise Manager™ Installation and User Guide, describes guide conventions, and lists other useful publications.

INTRODUCTION

This guide provides the required information to install and use the ExtremeWare Enterprise Manager software. It is intended for use by network managers who are responsible for monitoring and managing Local Area Networks, and assumes a basic working knowledge of:

- Local Area Networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- The Simple Network Management Protocol (SNMP)

Note: *If the information in the Release Notes shipped with your software differs from the information in this guide, follow the Release Notes.*

TERMINOLOGY

When features, functionality, or operation is specific to a particular model of the Summit family, the model name is used (for example, Summit1 or Summit4). Explanations of features and operations that are the same among all members of the Summit family simply refer to the product as the Summit.

CONVENTIONS

Table 1 lists conventions that are used throughout this guide.

Table 1: Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen .
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names appear in text in one of two ways. They may be <ul style="list-style-type: none">■ referred to by their labels, such as “the Return key” or “the Escape key.”■ written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). For example: Press [Ctrl]+[Alt]+[Del].
Words in bold type	Bold text indicates a button or field name.
Words in <i>italicized</i> type	Italics emphasize a point or denote new terms at the place where they are defined in the text.

RELATED PUBLICATIONS

The ExtremeWare Enterprise Manager documentation set includes the following:

- The ExtremeWare Enterprise Manager 2.0 User Guide (this manual)
- ExtremeWare Enterprise Manager 2.0 Release Notes
- ExtremeWare Enterprise Manager License Agreement

Other manuals that you will find useful are:

- ExtremeWare 4.0 Software User Guide
- ExtremeWare 4.0 Quick Reference Guide
- ExtremeWare Command Reference
- ExtremeWare 5.0 Release Notes
- The Summit Hardware Installation Guide
- BlackDiamond Hardware Installation Guide
- BlackDiamond User Guide
- The Summit Virtual Chassis Design and Installation Guide

The Extreme Networks web site provides much useful information:

- For general information about Extreme Networks, see the Extreme Networks home page:

<http://www.extremenetworks.com>

- A link to the ExtremeWare Enterprise Manager User Guide in PDF format may be found at:

<http://www.extremenetworks.com/support/documentation.htm>

- For a general description of ExtremeWare Enterprise Manager, and a link to a downloadable evaluation version of ExtremeWare Enterprise Manager version 2.0, go to:

<http://www.extremenetworks.com/products/datasheets/nms.htm>

- Customers with a support contract can access the Technical Support pages at:

<http://www.extremenetworks.com/support/database.htm>

The technical support pages provide the latest information on Extreme Networks software products, including the latest Release Notes, information on known problems, downloadable updates or patches as appropriate, and other useful information and resources.

1

ExtremeWare Enterprise Manager Overview

This chapter describes:

- Features of the ExtremeWare Enterprise Manager™
- ExtremeWare Enterprise Manager components
- Hardware and software requirements

INTRODUCTION

Today's corporate networks commonly encompass hundreds or thousands of systems, including individual end user systems, servers, network devices such as printers, and internetworking systems. Extreme Networks™ recognizes that network managers have different needs, and delivers a suite of ExtremeWare™ management tools to meet those needs.

The ExtremeWare Enterprise Manager is a powerful yet easy-to-use application suite that facilitates the management of a network of Summit™ and BlackDiamond™ switches, as well as selected third-party switches. ExtremeWare Enterprise Manager makes it easier to perform configuration and status monitoring, create virtual LANs (VLANs), and implement policy-based networking in enterprise LANs with Extreme Entreats switches. Leveraging ExtremeWare's powerful Policy-Based Quality of Service (QoS) capabilities, ExtremeWare Enterprise Manager offers a comprehensive set of network management tools that are easy to use from a workstation with a Java-enabled web browser.

The ExtremeWare Enterprise Manager leverages the three-tier client/server architecture framework represented by Java applets, and can be accessed using any Java-enabled browser. The Enterprise Manager application and database support two of the most popular operating environments in the marketplace, Microsoft Windows NT and Sun Microsystems' Solaris. Integration with HP OpenView provides additional flexibility.

SUMMARY OF FEATURES

In large corporate networks, network managers need to manage systems “end to end.” The ExtremeWare Enterprise Manager is a powerful, flexible and easy-to-use application for centralizing the management of a network of Extreme switches and selected third-party devices, regardless of the network size.

- **Enterprise-wide management.** The ExtremeWare Enterprise Manager software provides configuration and monitoring of Extreme Networks' switches and selected third-party devices anywhere within the enterprise network.
- **Multi-platform capability.** The ExtremeWare Enterprise Manager Server supports both Sun SPARC/Solaris and Intel/Windows NT.
- **Support for multiple users with security.** Users must log in to the application, and can be granted different levels of access to the application features.
- **Integration with HP OpenView.** The ExtremeWare Enterprise Manager client can be launched from within the HP OpenView Network Node Manager application.
- **Web-based client.** The Java-based client applets run under Netscape Navigator or Microsoft Internet Explorer.

You can set VLAN configuration and policy-based Quality of Service policies across the network. Centralized and distributed stacks of Summit switches can be managed as aggregated entities. Extreme Networks switches and selected Cisco devices can be monitored and controlled from a central web-based interface, without exiting ExtremeWare Enterprise Manager to run a separate program or telnet session. Features such as SmartTraps™ further maximize network monitoring capability while maintaining network usage efficiency.

EXTREMEVIEW CONFIGURATION AND STATUS MONITORING

With ExtremeView, any Extreme Networks switch can be monitored and controlled from a central, web-based platform, without leaving the ExtremeWare Enterprise Manager client to invoke another program or Telnet session.

The ExtremeView applet displays detailed information about the status of Extreme switches (Summit and Black Diamond switches) in a number of categories. Any Enterprise Manager user can view status information about these network devices known to the Enterprise Manager. Users with the appropriate access permissions can also view and modify configuration information for those switches using either the ExtremeWare Vista graphical user interface, or through Telnet and the ExtremeWare Command Line Interface (CLI). The ExtremeView Telnet feature includes a macro capability that lets you create and execute scripts of CLI commands repeatedly on multiple devices in one operation.

You can also use the interactive Telnet capability to view and modify configuration information for Cisco devices.

ENTERPRISE-WIDE VLAN MANAGEMENT

A virtual LAN (VLAN) is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN).

The ExtremeWare Enterprise Manager VLAN Manager is an enterprise-wide application that manages many aspects of VLANs on Extreme Network's Summit and BlackDiamond switches. Any Enterprise Manager user can view status information about the VLANs currently known to Enterprise Manager. Users with the appropriate access can create and delete VLANs, add and remove ports from existing VLANs, and create and modify the protocol filters used to filter VLAN traffic.

SUPPORT FOR SUMMIT VIRTUAL CHASSIS STACKS

The Summit™ Virtual Chassis™ is a high performance, low cost external backplane that connects up to eight stacked or distributed Summit switches into one cohesive system. A Virtual Chassis (VC) stack is a configuration of one to four Summit Virtual Chassis and up to eight connected Summit switches.

The Virtual Chassis Stack Manager of the ExtremeWare Enterprise Manager identifies and manages virtual stack configurations, including configuration of the Gigabit Ethernet ports on Summit switches. Any Enterprise Manager user can view the VC stack configuration topology and the details about individual components. Users with appropriate access can create, modify, and delete Virtual Chassis stack topology representations in the Enterprise Manager database, configure switch ports, and invoke a stack rediscovery.

POLICY-BASED QUALITY OF SERVICE

Policy-based management is used to protect and guarantee delivery of mission-critical traffic. A network policy is a set of high-level rules for controlling the priority of, and amount of bandwidth available to, various types of network traffic. Leveraging ExtremeWare 5.0's Policy-Based Quality of Service (QoS) capabilities, the ExtremeWare Enterprise Manager Policy System offers a powerful set of easy-to-use policy management tools that meet the application-specific needs of today's networks. Through ExtremeWare Enterprise Manager's Policy System Client, policies can be defined in terms of individual applications, users and desktop systems, not just by IP or MAC addresses.

The ExtremeWare Enterprise Manager Policy System lets you work with high-level policy objects (users, desktop systems, groups of users or systems, applications, and groups of devices and ports) in defining policies. The policy system translates those policy objects into the specific information needed for QoS configuration of network devices. It also detects overlaps and conflicts in policies, with precedence rules for resolving conflicting QoS rules.

To facilitate policy-setting based on user names or individual desktop systems, the Policy System takes advantage of the Dynamic Link Context System (DLCS) to map a user's name or system to the associated IP and MAC addresses.

The policy system also supports limited policy configuration for third-party devices—specifically selected Cisco devices and Xedia switches as of ExtremeWare Enterprise Manager release 2.0.

SIMPLE INVENTORY MANAGEMENT

The ExtremeWare Enterprise Manager's Inventory Manager applet keeps a database of all the devices managed by the Enterprise Manager. Any Enterprise Manager user can view status information about the switches currently known to Enterprise Manager.

The ExtremeWare Enterprise Manager 2.0 software provides an automatic discovery function. Users with the appropriate access can use this feature to discover Extreme, Cisco, and Xedia devices by specific IP address or within a range of IP addresses.

Network devices can also be added to the Enterprise Manager database manually, using the Inventory Manager Add function. Once a network device is known to the Enterprise Manager database, you can assign it to a specific device group, and configure it using the VLAN Manager, Virtual Chassis Stack Manager, ExtremeView, or the Policy System.

REAL-TIME STATISTICS

The Real-Time Statistics feature of ExtremeWare Enterprise Manager provides a graphical presentation of utilization and error statistics for Extreme switches in real time. The data is taken from Management Information Base (MIB) objects in the etherHistory table of the Remote Monitoring (RMON) MIB. You can choose from a variety of styles of charts and graphs as well as a tabular display.

You can view data for multiple ports on a device, device slot, or within a port group, optionally limiting the display to the “top N” ports (where N is a number you can configure). You can also view historical statistics for an individual port. If you choose to view a single port, the display shows the value of the selected variable(s) over time, and can show utilization history, total errors history, or a breakdown of individual errors.

THE MAC/IP ADDRESS FINDER

The IP/MAC Address Finder applet lets you search for network addresses (MAC or IP addresses) and identify the Extreme Networks switch and port on which the address resides.

SECURITY MANAGEMENT

In order to access the ExtremeWare Enterprise Manager features, a user must log in with a user name and a password.

The Enterprise Manager provides three access levels:

- Monitor—users who can view status information.
- Manager—users who can modify device parameters as well as view status information.
- Administrator—users who can create, modify and delete Enterprise Manager user accounts as well as perform all the functions of a user with Manager access.

ExtremeWare Enterprise Manager user accounts are separate from the Extreme switch user accounts. You can configure both through the Enterprise Manager, or you can have switch access independently of the Enterprise Manager.

You can use the Enterprise Manager and its Remote Authentication Dial In User Service (RADIUS) server to configure access permissions for Extreme switches. Two levels of access to Extreme switches can be enabled:

- User—users who can view device status information and statistics, but cannot modify any parameters.
- Administrator—users who can modify device parameters as well as view status information and statistics.

These permissions enable access to Extreme Networks switches through Telnet or ExtremeWare Vista. The use of the RADIUS server avoids the need to maintain user names, passwords, and access permissions in each switch, and instead centralizes the configuration in one location in the ExtremeWare Enterprise Manager.

EXTREMEWARE ENTERPRISE MANAGER COMPONENTS

The ExtremeWare Enterprise Manager software is made up of three major functional components:

- The ExtremeWare Enterprise Manager Server, which is based on the Sun Java Web Server. The server is responsible for downloading applets, running servlets, managing security, and communicating with the database.
- A Relational Database Management System (RDBMS), Sybase Adaptive Server Anywhere, which is used as both a persistent data store and a data cache.
- The ExtremeWare Enterprise Manager client applications, which are Java applets that are downloaded from the server to a client machine on request and executed in a Java-enabled web browser that supports Java 1.1.

Figure 1-1 illustrates the architecture of the ExtremeWare Enterprise Manager software.

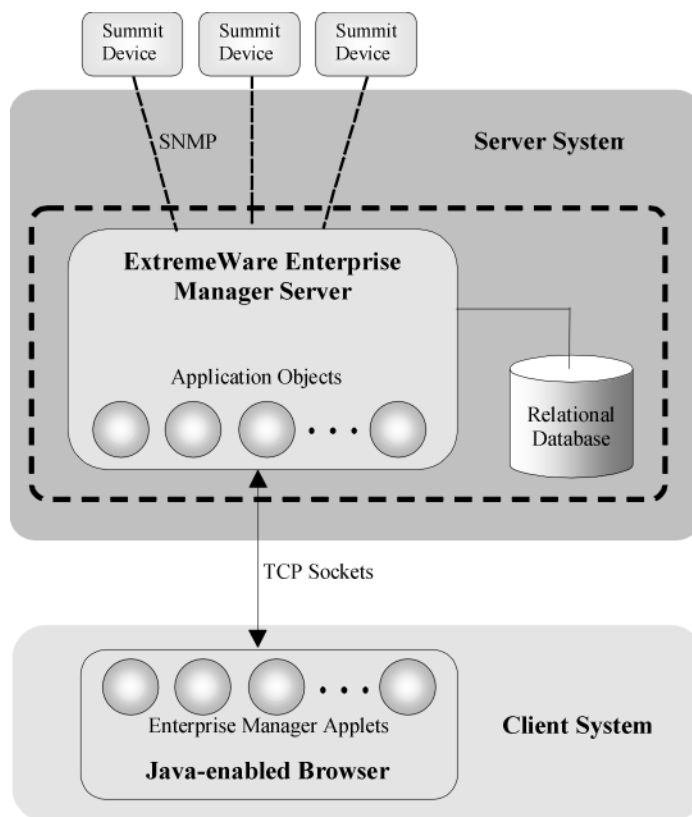


Figure 1-1: ExtremeWare Enterprise Manager software architecture

EXTREME NETWORKS SWITCH MANAGEMENT

ExtremeWare Enterprise Manager uses SNMP to monitor and manage the Extreme switches in the network. To avoid the overhead of frequent device polling, the ExtremeWare Enterprise Manager uses a mechanism called SmartTraps to identify changes in device status and configuration.

When an Extreme switch is added to the ExtremeWare Enterprise Manager database, the Enterprise Manager creates a set of SmartTraps rules that define what events (status and configuration changes) the Enterprise Manager needs to know about. These rules are downloaded into the Extreme switch, and the Enterprise Manager is automatically registered as a trap receiver. Subsequently, whenever a status or configuration change

takes place, the ExtremeWare software in the switch uses the SmartTraps rules to determine if the Enterprise Manager should be notified. These changes can be changes in device status, such as fan failure or overheating, or configuration changes made on the switch through the ExtremeWare CLI or ExtremeWare Vista.

The ExtremeWare Enterprise Manager does a “heartbeat” check, by default every five minutes, of all the switches it is managing to determine if the devices are still accessible. The ExtremeWare Enterprise Manager also provides you with the ability to explicitly gather device status at any time using the **Sync** feature in the Inventory Manager applet.

HARDWARE AND SOFTWARE REQUIREMENTS

The following sections specify the hardware and software you need to run the ExtremeWare Enterprise Manager software.

EXTREME NETWORKS DEVICE REQUIREMENTS

The ExtremeWare Enterprise Manager can manage Extreme Networks Summit and BlackDiamond switches running the ExtremeWare software release 2.0 or later within the switch. However, features such as the Policy-Based Management Service require ExtremeWare 5.0 or later.

THIRD-PARTY DEVICE REQUIREMENTS

ExtremeWare Enterprise Manager version 2.0 supports Cisco and Xedia devices as well as Extreme Networks switches.

Cisco devices require IOS 11.2 or later. Cisco 2500, 3600, 4000 and 7505 devices have been tested ExtremeWare Enterprise Manager Release 2.0.

Xedia devices require Xedia software 2.1. The Xedia Access Point switch has been tested with ExtremeWare Enterprise Manager 2.0.

See the *ExtremeWare Enterprise Manager Release Notes* for the most current list of qualified third-party devices.

SERVER REQUIREMENTS

The ExtremeWare Enterprise Manager Server can run under Microsoft Windows NT or Sun Microsystems' Solaris Operating Environment, SPARC Platform Edition.

For installation under Windows NT, the requirements are:

- Microsoft Windows NT 4.0 running on an Intel platform
- 128 MB RAM (256 MB recommended)
- Disk space depends on the file system used on the disk:
 - 200 MB disk space if the disk is using the NT File System (NTFS)
 - 20% of the disk if the disk is using the FAT file system (i.e 200MB on a 1 GB disk, 400 MB on a 2GB disk and so on)

You can tell the type of file system by looking at the disk properties.

- 200 Mhz Pentium-compatible processor
- CDROM drive (for installation)
- A network connection

For installation under Solaris, the requirements are:

- Solaris Operating Environment 2.6 or Solaris 7, with patches as specified below
- 128 MB RAM (256MB recommended)
- 200 MB disk space
- CDROM drive (for installation)

Required patches for Solaris 2.6:

Patch Number	Description
105181-11	Recommended kernel update
105210-17	Required libc patch
105490-05	Required linker patch
105568-13	Threads bug fix - prevents hanging
105633-18	Xserver font fixes
105669-04	Recommended - CDE 1.2 libDTSvc patch

Required patches for Solaris 7:

Patch Number	Description
106984-04	libthread patch
107078-03	OpenWindows 3.6.1 Xsun patch

ExtremeWare Enterprise Manager also provides software to enable you to launch the Enterprise Manager client from within HP OpenView, either from the Tools menu or from a pop up menu from the Network Node Manager map.

HP OPENVIEW REQUIREMENTS

The requirements for integration with HP OpenView are the following:

- HP OpenView release 5.01 or later under Microsoft Windows NT 4.0 or Solaris 2.6 or Solaris 7
- A Java-enabled browser (see Client Requirements)

CLIENT REQUIREMENTS

The client can run using the following browsers:

- Microsoft Internet Explorer version 4.72 or later under Windows 95 or Windows NT, with the 5.0 JVM. Microsoft Internet Explorer 5.0 is recommended.
- Netscape Navigator version 4.0.7 and later under SPARC Solaris (2.5.1, 2.6, or 7) or HPUX 10.20

The client system must have a monitor that supports 800x600 resolution and at least 256 colors (16-bit color is recommended).

Note: See the ExtremeWare Enterprise Manager Release Notes *shipped with the software for the latest information about configuration requirements.*

2

Installing the ExtremeWare Enterprise Manager

This chapter describes how to do the following:

- Install the ExtremeWare Enterprise Manager Server under either Windows NT or the Solaris Operating Environment
- Install the browser-based client software

INSTALLATION OVERVIEW

The ExtremeWare Enterprise Manager software includes a set of Java applications, a Web Server, and database software. The installation process installs all of these components on a Windows NT or a SPARC-based system running the Solaris Operating Environment.

The ExtremeWare Enterprise Manager client runs in a Java-enabled browser. It can be either be accessed remotely, with each module downloaded from the Enterprise Manager server as required, or the client applet can be installed locally on the client system. Local installation will speed up the process of loading each of the modules, compared to downloading them from the server.

The HP OpenView integration process makes it possible to launch the ExtremeWare Enterprise Manager client from within HP OpenView. The Enterprise Manager can be launched from the HP OpenView Network Node Manager Tools menu, or from an icon on the Network Node Manager toolbar.

The ExtremeWare Enterprise Manager client runs within a Java 1.1-enabled browser.

Note: See the ExtremeWare Enterprise Manager Release Notes for the most current information on installation requirements.

The ExtremeWare Enterprise Manager server installation process installs two components:

- The ExtremeWare Enterprise Manager Database Engine
- The ExtremeWare Enterprise Manager Web Server

INSTALLING ON A WINDOWS NT SYSTEM

The following sections assume that Microsoft Windows NT is already running.

Note: For information on installing and running Windows NT, refer to the documentation supplied with your Microsoft Windows NT software.

INSTALLING THE ENTERPRISE MANAGER SERVER

To install the ExtremeWare Enterprise Manager components under Windows NT you must have Windows NT administrator privileges.

If you have a previous release of ExtremeWare Enterprise Manager installed (1.0 or 1.1) the installation script will also handle migrating your database information to the new Enterprise Manager 2.0 installation.

Note: To update an evaluation copy of the Enterprise Manager to a licensed copy without reinitializing the database, follow the update procedure described in the section "Updating an Evaluation Version to a Licensed Version."

To install the ExtremeWare Enterprise Manager, follow these steps:

- 1 Close any open applications.
- 2 Insert the CDROM into the CDROM drive.
- 3 In most cases, the ExtremeWare Enterprise Manager Welcome screen appears automatically. If it does not:
 - a Choose **Run** from the Start Menu.
The Run dialog box appears.
 - b Type **d:\nt\setup** in the text box and click **OK**.
If the CDROM is not drive **d**, substitute the correct drive letter.

The ExtremeWare Enterprise Manager Welcome screen appears.

- 4 Follow the on-screen instructions to progress through the Welcome screen.
- 5 If you are running a previous version of ExtremeWare Enterprise Manager, you are notified that the EEM 1.x services will be stopped in order to install EEM 2.0. If this is acceptable, click **Yes**.
- 6 Click **Yes** to accept the license agreement.
- 7 Enter your company information.
- 8 Enter your license key.
 If this is an evaluation copy, accept the default license key, Evaluation. This allows you to use the product for 30 days.
 If this is a fully-licensed copy, enter the license key found on the License Agreement that came with the software.
- 9 In the Destination dialog box, choose one of two options:
 - Accept the default target drive and folder displayed in the Destination Directory box.
 - Click **Browse** and select or enter a new folder, a new drive, or both.
 If you are installing on a disk that uses the FAT file system rather than the NTFS file system, a warning message pops up when you click **Next**. This is because the ExtremeWare Enterprise Manager software can take up as much as 20% of your partition, regardless of the size of the partition.
- 10 In the Installation Type dialog box, select the set of files to install:
 - Click **Typical Install** to install all the files provided with the ExtremeWare Enterprise Manager software.
 - Click **Custom Install** to specify which files to install. For ExtremeWare Enterprise Manager you must install all the components except the Multimedia Files.
- 11 Accept the default program folder, ExtremeWare Enterprise Manager 2.0, or select a different program folder and click **Next**.
- 12 In the Database Server Information dialog box, enter a number into the **Port** field for the port that the Enterprise Manager Web Server will use to communicate with the database, or accept the default (2638). You can use any port number (a number between 1024 and 9999 is recommended) except a port number already in use by another process.
- 13 In the Get HTTP Port dialog box, you are asked for three ports that the Enterprise Manager Web Server will use:

- The HTTP Port for communication with clients (default 80).
- The Admin Port used by the Enterprise Manager web server (default 9095).
- An Internal port used by the Enterprise Manger web server (default 9096).

Accept any or all of the default port numbers, or enter different port numbers. You can use any port number (a number between 1024 and 9999 is recommended) except:

- The port number you just entered for the database TCP port.
- Any port number already in use by another process.

14 To view an Extreme Networks on-screen video while the installation is taking place, click Yes. Click **No** to proceed without the on-screen video.

15 If you are upgrading from an earlier version of ExtremeWare Enterprise Manager, a notice appears advising you that the EEM services are being shut down.

Note: *If you have more than one previous version of ExtremeWare Enterprise Manager installed, the installation script will use the latest version to do the upgrade. If this is not what you want, you must uninstall all versions except the one you want to upgrade before you start the new installation.*

The installation software then copies the ExtremeWare Enterprise Manager program files from the CD to your system.

16 When the files are copied, the Install as a Service dialog box asks if you want to install the ExtremeWare Enterprise Manager database and web server components as a Windows NT service.

- Click **Yes** to install the Enterprise Manager components as services. This is strongly recommended. If the Enterprise Manger components run as services, they will be started automatically on system boot, and will persist across user logins and logouts.

Note: *You must have NT Administrator privileges to install the Enterprise Manager components as services.*

In addition, if you want to be able to import user and host information from a Windows NT Domain Controller, the ExtremeWare Enterprise Manager web server component must run with permissions that allow it to get user information from a Domain Controller.

- Click **No** if you do not want to install the components as services.

17 If you are upgrading from an earlier version of Enterprise Manager, you are asked whether you want to copy the database and other persistent data to the new installation. Click **Yes** to copy the data, or **No** to continue without doing so.

If you answer Yes, an MS-DOS window will appear briefly while the database contents are dumped from the old 1.x database and loaded into the 2.0 database.

- 18** If HP OpenView is installed on the system where you are installing the ExtremeWare Enterprise Manager server, the installation software asks if you want to integrate with HP OpenView. Integration allows access to the ExtremeWare Enterprise Manager and ExtremeWare Vista from the HP OpenView user interface.

If HP OpenView is installed, you can do the installation at this time.

If HP Openview is not installed on this system, you will not see this prompt. You can run the HP OpenView integration process separately on the system where HP OpenView is installed.

- To run the HP OpenView integration process now, click **Yes**. Then go to “Integrating with HP OpenView under Windows NT” in Appendix A and follow the instructions.
- To skip the HP OpenView integration process, click **No**.

- 19** If you want to view the Readme file, click the check box, then click **Finish** to complete the installation process.

- 20** Finally, you are asked whether you want to reboot your system. If you choose not to do so at this time, you must reboot the server before you can run the ExtremeWare Enterprise Manager server software.

UPDATING AN EVALUATION VERSION TO A LICENSED VERSION

To update an evaluation copy of the ExtremeWare Enterprise Manager to a fully-licensed copy, use the utility provided.

Note: *DO NOT reinstall the software if you have any data or configurations of value in the Enterprise Manager database. Re-installation will re-initialize the database.*

To update an evaluation copy, follow these steps:

- 1** Click **Start**.
- 2** Highlight **Programs** to display the Programs menu.
- 3** Highlight **Command Prompt** in the Programs menu to display a command window.
- 4** Enter the command `<install_dir>/instlic <key>`

`<install_dir>` is the directory (path) where you installed the Enterprise Manager components. If you installed in the default directory, the path is

`c:\EEM2_0\`

`<key>` is the 11-character license key found on the License Agreement shipped with the ExtremeWare Enterprise Manager software. Type the key exactly as it is shown on the License Agreement.

If the license update is successful, the message “License Installed” is displayed.

If the update is not successful, the message “Invalid argument key : `<key>`” is displayed. `<key>` is the license key you entered with the `instlic` command. Verify that you typed the key exactly as shown on the license agreement.

UNINSTALLING THE ENTERPRISE MANAGER SERVER

To uninstall the ExtremeWare Enterprise Manager from a Windows NT system, follow these steps:

- 1 From the **Start** menu, highlight **Settings**, pull right, and click on the **Control Panel**. This displays the Control Panel folder.
- 2 Shut down the Enterprise Manager components if they are still running.
 - If they are running as services, double-click on **Services** to display the Services Properties window, and stop both the EEM Web Server and EEM Database Engine. You must have NT Administrator privileges to access this function.
 - If they are running as regular applications, open the **ExtremeWare Enterprise Manager 2.0 Server** MS-DOS window (from the Task bar) and type [Ctrl]+C at the DOS command prompt to shut down the Enterprise Manager Web Server. To shut down the **Sybase Adaptive Server Anywhere**, open the window found on the Windows Task bar at the far right (a small “SQL” in red and yellow letters) and click **Shutdown**.
- 3 From the Control Panel folder, double-click **Add/Remove Programs**. This displays the **Add/Remove Program Properties** window.
- 4 From the list of installed programs, select **ExtremeWare Enterprise Manager 2.0** and click **Add/Remove**. Follow the instructions to remove the component.

INSTALLING ON A SPARC SOLARIS SYSTEM

ExtremeWare Enterprise Manager server software version 2.0 is supported under Solaris 2.6 or Solaris 7. Each of these operating environments require patches for ExtremeWare Enterprise Manager to function properly. The following sets of patches are required. Make certain these patches have been installed before you install the ExtremeWare Enterprise Manager server software.

For the most current information on required patches, see the *ExtremeWare Enterprise Manager Release Note* that accompanies your ExtremeWare Enterprise Manager software.

Patches for Solaris 2.6:

Patch Number	Description
105181-11	Recommended kernel update
105210-17	Required libc patch
105490-05	Required linker patch
105568-13	Threads bug fix - prevents hanging
105633-18	Xserver font fixes
105669-04	Recommended - CDE 1.2 libDTSvc patch

Patches for Solaris 7:

Patch Number	Description
106984-04	libthread patch
107078-03	OpenWindows 3.6.1 Xsun patch

The following sections assume that you are running in a command shell or Xterm window.

INSTALLING THE ENTERPRISE MANAGER SERVER

You can install the Enterprise Manager components without being logged in as root, as long as you do not use port numbers less than 1024 (for example, port 80 for the Enterprise Manager Web server, which is the default).

Note: *When you install the Enterprise Manager Server, it initializes the database. If you attempt to re-install the server once you have installed it, the installation process reinitializes the database, and your existing data and configurations will be lost.*

To update an evaluation copy of the Enterprise Manager to a licensed copy without reinitializing the database, follow the update procedure described in the section "Updating an Evaluation Version to a Licensed Version."

To install the ExtremeWare Enterprise Manager server software, follow these steps:

- 1 Insert the CDROM into the CDROM drive.
- 2 If you are running CDE, the contents of the CDROM are displayed in the File Manager. Go to the **solaris** directory.

To run from an Xterm window:

```
cd /cdrom/eem2_0/solaris
```

- 3 Run the installation script:

```
./install.sh
```

The ExtremeWare Enterprise Manager Welcome message appears as follows:

```
*****
```

```
Welcome to the Extreme Networks ExtremeWare Enterprise Manager
install program. This program will install:
ExtremeWare Enterprise Manager version 2.0.0 on this system.
```

```
*****
```

```
Please review the following software license terms
and conditions. You will need to accept this license
to continue the installation. Press space to page
through the license.
Press <enter> to view the license:
```

- 4 When you press enter, the text of the license is displayed. You can use the space bar to page through it. When you reach the end, you are asked:

```
Do you agree to the above conditions? (Y/N):
```

- 5 Enter **Y** if you agree and want to proceed. Enter **N** to terminate the installation process. This question does not have a default, you must enter Y or N.

- 6 Next, you are prompted for the directory where the ExtremeWare Enterprise Manager server software should be installed:

```
Please enter the directory in which the software will be installed.
The default directory is /opt/eem20, but the product may be
installed anywhere.
```

```
Install Directory [/opt/eem20]:
```

Enter the directory or accept the default (/opt/eem20).

If you specify a directory that does not exist, you are asked whether it should be created:

```
/opt/eem20: No such directory. Do you wish to create it? (y/n)[y]
```

Assuming you want to create the directory, accept Y as the default. If you answer N, the script will assume the directory already exists.

7 The installation script now copies and installs the ExtremeWare Enterprise Manager files:

```
Installing ExtremeWare Enterprise Manager files...
```

After copying a number of files, the following message appears:

```
File copy complete.
Configuring Installation.
```

At this point additional files are copied and the ExtremeWare Enterprise Manager installation tree is created, and filled out. This will take several minutes.

When the files are complete, you are asked for a set of configuration information.

To configure ExtremeWare Enterprise Manager (EEM), we will need to ask you for some information. In most case the default answers will work correctly.

8 First you are asked whether you want to upgrade from a previous version of ExtremeWare Enterprise Manager.

```
*** Upgrade Parameters
```

If there is a previous installation of EEM installed, you may import the database and the license from the previous installation. If there is no previous install, or you would like to start from scratch, select new installation.

```
Would you like to upgrade from a previous install? (Y/N) [N]:
```

Answer Y to upgrade.

If you answer Yes, the install script asks for the location of the previous version of ExtremeWare Enterprise Manager.

```
Old install directory [/opt/eem]: /opt/eem1.1
```

Accept the default or enter the actual location (full path name).

9 Next, you are asked for a license key.

```
*** License Key
```

Please enter the license key for the product.

For purchased products, this is found on the license agreement sheet included with the product.
'Evaluation' will grant a 30 day evaluation license.

Please enter the license key: [Evaluation]

If you have purchased the product and received a license key from Extreme Networks, enter it here. If you are installing an evaluation copy, accept the default, Evaluation.

10 Next, you are asked to enter a port for communication between the Web server and the database server:

*** Database Parameters

EEM will run an SQL database server on this machine. The database needs the name of this machine and an unused port to listen on.

Please enter the port for the database: [2638]

Accept the default (2638) for the port that the Enterprise Manager Web Server will use to communicate with the database, or enter a different port number. You can use any port number (a number between 1024 and 9999 is recommended) except a port number already in use by another process.

11 You are now asked for three ports that the Enterprise Manager Web Server will use.

*** Web Server Parameters

EEM runs as a web server and by default accepts HTTP requests on port 80. You may specify an alternative. Additionally EEM needs two other unused ports, one for a web administrative server and one for internal usage. If you are not sure what to enter, the defaults should be acceptable.

Please enter the http port for the web server: [80]

Please enter the http port for the admin web server: [9090]

Please enter the http port for the web server: [9091]

Accept any or all of the default port numbers, or enter different port numbers. You can use any port number (a number between 1024 and 9999 is recommended) except:

- The port number you just entered for the database TCP port.

— Any port number already in use by another process.

12 Finally, you are asked to confirm the configuration parameters:

```
*** Configuration
```

Please review the following items.

```
Upgrade                = NO
License                = <the key you entered or "Evaluation">
Database Port          = <the port you entered or 2638>
HTTP Port              = <the port you entered or 80>
HTTP Admin Port        = <the port you entered or 9090>
HTTP Internal Port     = <the port you entered or 9091>
```

Are these correct? (Y to accept / N to re-enter) [N]:

13 If you accept the parameters by entering Y, the installation script will finish with the following messages:

```
Installing License...
License installed.
Done.
```

```
Updating
./WebServer/properties/server/javawebserver/webpageservice/servlets.pr
operties
```

```
Updating
./WebServer/properties/server/javawebserver/webpageservice/endpoint.pr
operties
```

```
Updating
./WebServer/properties/server/adminserver/adminservice/admin_port.prop
erties
```

```
Updating
./WebServer/properties/server/javawebserver/adminservice/admin_port.pr
operties
```

```
Updating ./WebServer/properties/server/javawebserver/server.properties
/space/opt/eem20
```

If you are upgrading from an earlier version of ExtremeWare Enterprise Manager, you will also see the following:

```
*** Database Upgrade
```

```
Upgrading Database...
```

```
Upgrading from EEM 1.1
```

```
Generating sql files...
```

```
Dumping data from tables in old database ...
```

```
Loading data into tables in new database ...
```

```
Database Upgrade Complete.
```

The final messages are:

```
The ExtremeWare Enterprise Manager software installation is complete.
```

```
To start the server, run /opt/eem20/runserv &
```

Once the server is running, you can run the client in a supported web browser with the following URL:

```
http://<host>:<port>/
```

<host> and *<port>* are the name of the system you've just installed on, and the HTTP port you entered (or 80 if you accepted the default).

UPDATING AN EVALUATION VERSION TO A LICENSED VERSION

To update an evaluation copy of the ExtremeWare Enterprise Manager to a fully-licensed copy, use the utility provided.

Note: *DO NOT reinstall the software if you have any data or configurations of value in the Enterprise Manager database. Re-installation will re-initialize the database.*

- Set the current directory to the Enterprise Manager installation directory and run the installation script:

```
<install_dir>/instlic <key>
```

<install_dir> is the directory (path) where you installed the Enterprise Manager components.

For example, if you installed in the default directory, enter:

```
/opt/eem20/instlic <key>
```

<key> is the 11-character license key found on the License Agreement shipped with the ExtremeWare Enterprise Manager software. Type the key exactly as it is shown on the License Agreement.

If the license update is successful, the message “License Installed” is displayed in the xterm or command window.

If the update is not successful, the message “Invalid argument key : <key>” is displayed. <key> is the license key you entered with the `instlic` command. Verify that you typed the key exactly as shown on the license agreement.

UNINSTALLING THE ENTERPRISE MANAGER SERVER

To remove the ExtremeWare Enterprise Manager server software from a Solaris host, stop the server using the **stopserv** command, then remove the all the files in the installation directory.

To remove the Enterprise Manager server software, follow these steps:

- 1 Run the **stopserv** command found in the root installation directory.

The installation directory is the directory (path) where you installed the Enterprise Manager components.

For example, if you installed in the default directory, enter:

```
/opt/eem20/stopserv
```

This shuts down the Enterprise Manager server if it is running.

- 2 Make the parent of the installation directory the current directory, and remove all files from the directory and its sub-directories.

For example, if you installed using the default directory path, `/opt/eem20`, enter:

```
cd opt
```

- 3 Remove all files from the installation directory tree.

For example, if you installed using the default directory path, enter:

```
rm -rf eem20
```

This removes all the Enterprise Manager components, including the database, from the system.

INSTALLING THE ENTERPRISE MANAGER CLIENT

In order to run the ExtremeWare Enterprise Manager client, Web browser software must be installed.

- Under Windows 95 or Windows NT, install Microsoft Internet Explorer 5.0 with the Microsoft 5.x JVM.

To download Internet Explorer 5.0, go to

<http://www.microsoft.com/ie/>

The Enterprise Manager client will also run with Internet Explorer 4.0 with the Microsoft 5.x JVM. Versions of Internet Explorer earlier than 4.72.3110.8 (as displayed in **About Internet Explorer** from the **Help** menu) may have slow performance.

For JVM updates for Internet Explorer 4.0, go to

http://www.microsoft.com/java/vm/dl_vm32.htm

Under Solaris, install Netscape Navigator with the JDK 1.1 support update.

Navigator is included in Netscape Communicator, and both the Communicator and the JDK patch can be downloaded from Netscape Communications. Go to the Netscape developer web site at <http://developer.netscape.com/software/> for more information. From there you can find links to download the Communicator and the JDK 1.1 for the Communicator.

On Windows NT systems, the Enterprise Manager client software can be downloaded and installed on the client system, but does not *require* local installation. If you do not install it locally, it is downloaded into the browser automatically when you enter the URL of the Enterprise Manager Server.

DOWNLOADING THE CLIENT APPLLET IN INTERNET EXPLORER

If you are running Internet Explorer, you are given two choices for launching the Enterprise Manager client when you connect your browser to the ExtremeWare Enterprise Manager server. One of these choices is to run the ExtremeWare Enterprise Manager client locally on your system. To download the client applet to your system, do the following:

- 1 From your browser, enter the following URL:

<http://<host>:<port>/>

In the URL, replace *<host>* with the name of the system where the ExtremeWare Enterprise Manager server is running. Replace *<port>* with the TCP port number

that you assigned to the ExtremeWare Enterprise Manager Web Server during installation.

Note: If you used the default web server port, 80, you do not need to include the port number.

The Enterprise Manager Start-up page appears, as shown in Figure 2-1.

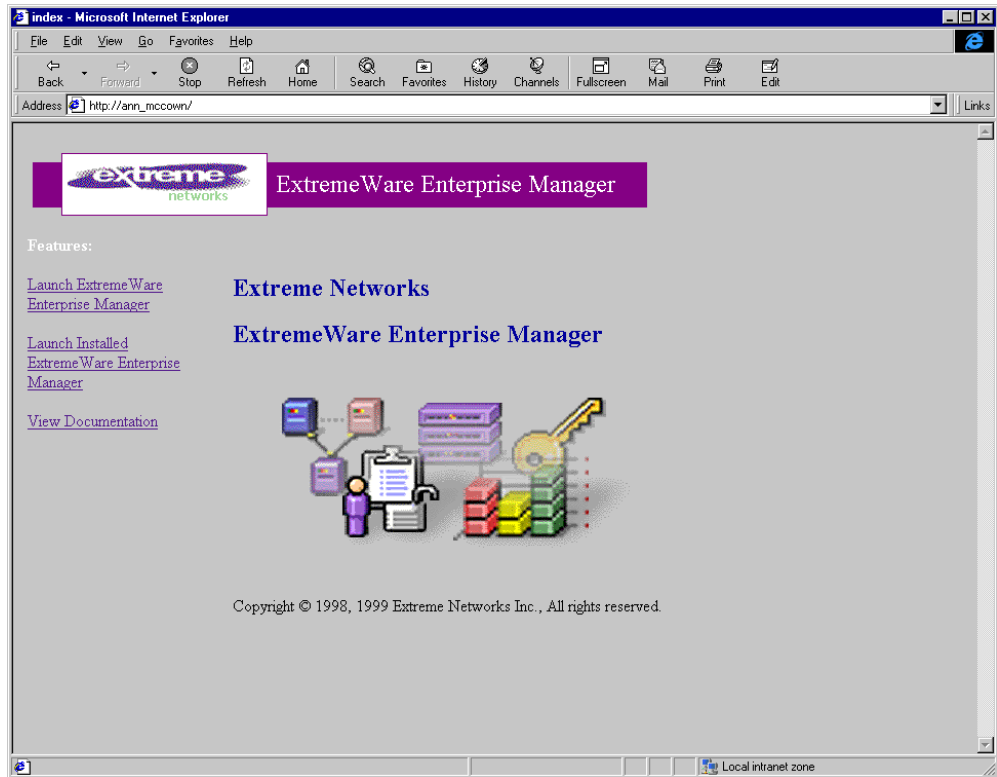


Figure 2-1: ExtremeWare Enterprise Manager Start-up page

- 2 From the Enterprise Manager Start-up page click **Launch Installed ExtremeWare Enterprise Manager**. The first time you choose this link, a page will pop up informing you that a signed applet is going to be downloaded (see Figure 2-2).

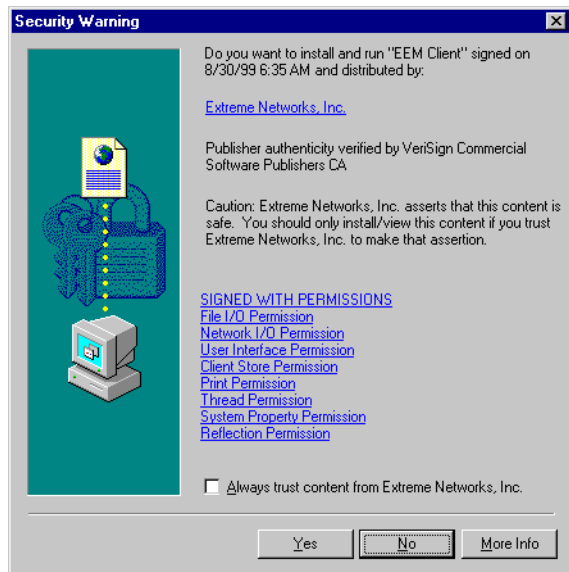


Figure 2-2: Security Warning prior to downloading the signed client applet

- 3 To continue with the download, click **Yes**.

To get more information about the applet, the security certificate or the permissions that are being granted, select any of the links on the page, or click the **More Info** button.

- 4 When the download is complete, the ExtremeWare Enterprise Manager Login page appears.

UNINSTALLING THE CLIENT APPLET

You can remove the downloaded client as follows:

- 1 From Internet Explorer, select **Internet Options...** from the **View** menu.
- 2 On the **General** tab, under the Temporary Internet Files section, click **Settings....**
- 3 Click **View Objects...** to display the Downloaded Programs window.
- 4 Find the entry for "EEM Client" and highlight it.
- 5 From the **File** menu, select **Remove Program File** to remove the client applet.

3

Starting the ExtremeWare Enterprise Manager

This chapter describes:

- Starting the ExtremeWare Enterprise Manager Server.
- Launching an Enterprise Manager Client.
- Navigating the Enterprise Manager pages.

When you log in for the first time after installing the ExtremeWare Enterprise Manager server software, there are only two user accounts enabled—an Administrator account “admin,” and a user account “user” with Monitor access privileges. Neither account has a password. Follow the instructions in Chapter 4 to change the admin password and to create additional Enterprise Manager user accounts.

RUNNING THE ENTERPRISE MANAGER UNDER WINDOWS

The following instructions assume that the Windows NT operating system is already running, and that the ExtremeWare Enterprise Manager server software is already installed.

If you have installed the ExtremeWare Enterprise Manager components as services under Windows NT, the Enterprise Manager Server and database component will start automatically when you boot the server. This is the recommended method of installing the ExtremeWare Enterprise Manager.

STARTING OR RESTARTING THE ENTERPRISE MANAGER SERVER

If you have not installed the components as a service, you must start them manually after you boot the server system. You can do this from the Windows NT Start menu.

The ExtremeWare Enterprise Manager Server consists of two components:

- The ExtremeWare Enterprise Manager Database Engine
- The ExtremeWare Enterprise Manager Web Server

Both components must be running in order to run the Enterprise Manager client applets.

To start the ExtremeWare Enterprise Manager Server and database components, follow these steps:

- 1 Click **Start**.
- 2 Highlight **Programs** to display the Programs menu.
- 3 Highlight **ExtremeWare Enterprise Manager** in the Programs menu to display the ExtremeWare Enterprise Manager menu.
- 4 Click **ExtremeWare Enterprise Server**. This runs `runserve.exe`, a program that starts the two components in the required order.

Two windows are displayed as the Enterprise Manager Server starts up:

- Sybase Adaptive Server Anywhere. This window is iconified and placed on the right side of the Windows task bar.
- A MS-DOS window that shows the processes being started.

SHUTTING DOWN THE ENTERPRISE MANAGER SERVER COMPONENTS

If the ExtremeWare Enterprise Manager components are running as services, follow these steps to shut them down:

- 1 From the **Start** menu, highlight **Settings**, pull right, and click on the **Control Panel**. This displays the Control Panel folder.
- 2 From the Control Panel folder, double-click **Services**. This displays the Services Properties window. You must have NT Administrator privileges to access this function.
- 3 From the list of installed programs select **EEM Web Server** and click **Stop**.

- 4 Repeat the same actions for the **EEM Database Engine**.

If the components are running as regular applications, follow these steps to shut them down:

- 1 Double-click on the **ExtremeWare Enterprise Manager 2.0 Server** button on the Windows Taskbar to bring up the **ExtremeWare Enterprise Manager 2.0 Server** MS-DOS window.
- 2 Type [Ctrl]+C at the DOS command prompt to shut down the Enterprise Manager Web Server.
- 3 Double-click on the small icon for the **Sybase Adaptive Server Anywhere** which is found on the Windows Taskbar at the far right (a small “SQL” in red and yellow letters).
- 4 When the window is displayed, click the **Shutdown** button to shut down the program.

RESTARTING THE ENTERPRISE MANAGER SERVER COMPONENTS AS SERVICES

To restart the ExtremeWare Enterprise Manager components as services, follow these steps:

- 1 From the Start menu, highlight **Settings**, pull right, and click on the Control Panel. This displays the Control Panel folder.
- 2 From the Control Panel folder, double-click **Services**. This displays the Services Properties window. You must have NT Administrator privileges to access this function.
- 3 From the list of installed programs select **EEM Database Engine** and click **Start**.
- 4 Repeat the same action for the **EEM Web Server**
- 5 If you want to change the start-up parameters, click **Startup...** instead of **Start**.

In order to import users from an NT Domain Controller, the EEM Web Server must be running with permissions that enable it to get user information from the Domain Controller. You can specify the log on account for the Web Server as a start-up parameter:

- In the **Log On As:** section of the **Startup...** pop up window, enter the account name and password for a user that has the appropriate permissions to access the Domain Controller.

RUNNING THE ENTERPRISE MANAGER UNDER SOLARIS

The following instructions assume that you are using a command or Xterm window running the C shell.

STARTING OR RESTARTING THE ENTERPRISE MANAGER SERVER

To run the Enterprise Manager Server:

- 1 Set the current directory:

```
cd <install_dir>
```

<install_dir> is the directory (path) where you installed the Enterprise Manager components. If you installed in the default directory, the path is `/opt/eem20`.

- 2 Invoke `runserve` to start the three Enterprise Manager components in the required order.

```
runserve &
```

SHUTTING DOWN THE ENTERPRISE MANAGER SERVER COMPONENTS

To shut down the Enterprise Manager Server:

- 1 Set the current directory:

```
cd <install_dir>
```

<install_dir> is the directory (path) where you installed the Enterprise Manager components. If you installed in the default directory, the path is `/opt/eem20`.

- 2 Invoke `stopserv` to shut down the Enterprise Manager components in the required order.

```
stopserv &
```

This shuts down the Enterprise Manager server if it is running.

LAUNCHING THE EXTREMEWARE ENTERPRISE MANAGER CLIENT

The Enterprise Manager client user interface is a Java-based application that runs within a Java-enabled browser such as Microsoft Internet Explorer 4.72 or later under Windows 95 or Windows NT, or Netscape Communicator (Navigator) version 4.0.7 or later under Solaris or HP-UX.

To run the ExtremeWare Enterprise Manager client interface:

- 1 Launch your Web browser.
- 2 Enter the following URL:

`http://<host>:<port>/`

In the URL, replace *<host>* with the name of the system where the ExtremeWare Enterprise Manager server is running. Replace *<port>* with the TCP port number that you assigned to the ExtremeWare Enterprise Manager Web Server during installation.

Note: *If you used the default web server port, 80, you do not need to include the port number.*

The Enterprise Manager Start-up page appears. Figure 3-1 shows the Start-up page on windows in Microsoft Internet Explorer. The Start-up page for Solaris under Netscape Navigator is similar.

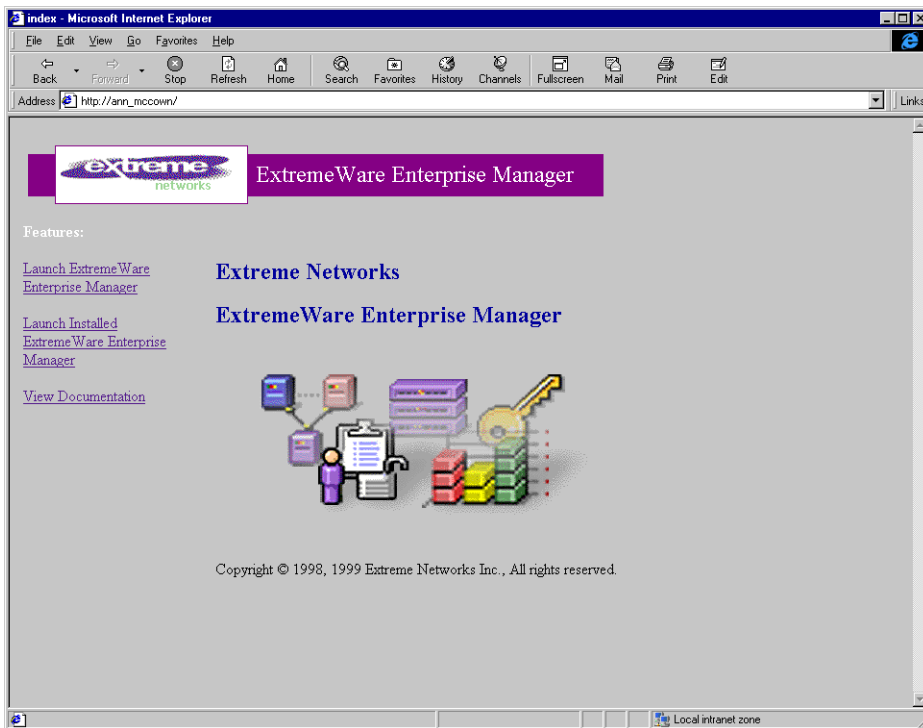


Figure 3-1: ExtremeWare Enterprise Manager Start-up page

3 You are presented with several ways to run the ExtremeWare Enterprise Manager client:

For Windows NT or Windows 95 running Internet Explorer:

- Click **Launch ExtremeWare Enterprise Manager** to launch the Enterprise Manager using the JVM in the browser.
- Click **Launch Installed ExtremeWare Enterprise Manager Client** to run the client applet locally. If the most current version of the client applet has not been downloaded, you will be prompted to download it (see “Installing the Enterprise Manager Client” in Chapter 2).

For Solaris or HP-UX running Netscape Navigator:

- Click **Launch ExtremeWare Enterprise Manager** to launch the Enterprise Manager using the JVM in the browser.

- Click **Launch ExtremeWare Enterprise Manager with the Java Plug-In** to launch the Enterprise Manager using Sun's Java plug-in. If the most current version of the plug-in is not available, you will be prompted to download it, and will be led through the brief installation process.

The ExtremeWare Enterprise Manager Login page appears, as shown in Figure 3-2.

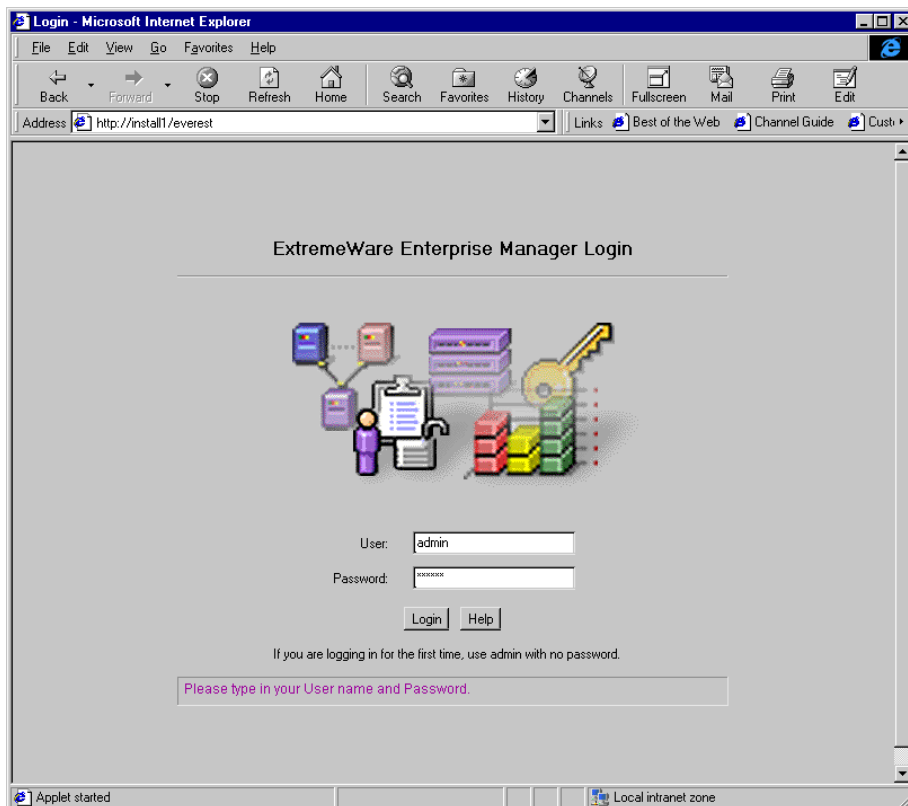


Figure 3-2: ExtremeWare Enterprise Manager Login page

Note: *There are two default user accounts—the Administrator account “admin,” and the user account “user” with Monitor access privileges. Initially, those accounts have no password. Chapter 4 describes how an Enterprise Manager Administrator can create additional Enterprise Manager user accounts.*

To log into ExtremeWare Enterprise Manager:

- 1 Type your user name in the **User** field if you already have an ExtremeWare Enterprise Manager user account.
 - If you are the network administrator logging in to the Enterprise Manager server for the first time since it has been installed, log in as “admin.”
You will be able to change the admin password (*strongly recommended*) and to create additional user accounts.
 - If you are a new user without your own account on the Enterprise Manager server, log in as “user.” You will be able to view information in the various modules, but will not be able to change any configurations.

- 2 Type your password in the **Password** field.

Both default names (user and admin) initially have no password, so you can leave the field blank.

- 3 Click **Login**.

If you are using an evaluation copy of the ExtremeWare Enterprise Manager, a dialog box appears notifying you how much longer the copy is valid.

Click **OK**.

The **About ExtremeWare Enterprise Manager** page appears.

NAVIGATING THE ENTERPRISE MANAGER FUNCTIONS

The ExtremeWare Enterprise Manager client consists of two frames, as shown in Figure 3-3.



Figure 3-3: The About ExtremeWare Enterprise Manager page

- The Navigation Toolbar, on the left, displays a set of buttons you can use to access various Enterprise Manager modules.
 - **About** returns you to the display shown in Figure 3-3.
 - **Inventory** runs the Inventory Manager.
 - **VLAN** runs the VLAN Manager.
 - **VC** runs the Virtual Chassis Stack Manager.
 - **Admin** runs the Administration module, where a user with Administrator access can administer ExtremeWare Enterprise Manager user accounts. Other users can change their own password using this applet.

- **EView** runs the ExtremeView applet.
- **Policy** runs the Policy System applet.
- **RT Stats** runs the Real Time statistics applet.
- **Find IP/MAC** runs the MAC/IP Address Finder applet.
- **Logoff** ends your session and returns you to the Login display.
- The main applet frame is used to display the active Enterprise Manager applet. For example, in Figure 3-4, the VLAN Manager is displayed in the main applet frame.

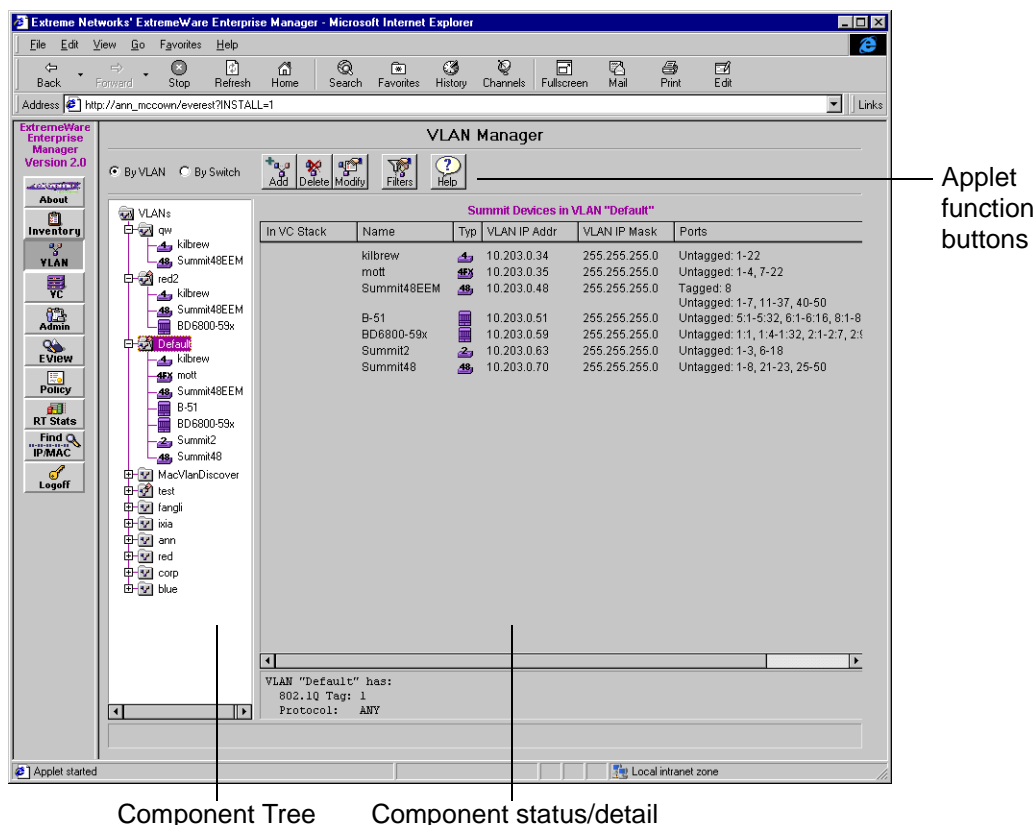


Figure 3-4: VLAN Manager applet running in a browser window

Enterprise Manager applets use a two-panel display within the main applet frame. The two panels are:

- The Component Tree.
- A component status/detail information panel.

In addition, some applets provide an applet-specific set of buttons at the top of the main applet frame. These provide access to specific applet functions, such as adding, deleting, or configuring components managed by the applet.

THE COMPONENT TREE

The left side panel shows the Component Tree. The Component Tree is a nested tree that displays the components known to the Enterprise Manager database that are relevant to the active module. The Component Tree displays different sets of components depending on which Enterprise Manager module you are viewing.

For example, in the Inventory Manager, the Component Tree shows all the Extreme and third-party devices known to the ExtremeWare Enterprise Manager. In the VLAN Manager, the Component Tree displays VLANs, as shown in Figure 3-4. In the Virtual Chassis Stack Manager, the Component Tree displays all the known Virtual Chassis stacks. In the Policy System client, the Component Tree shows the categories of elements you can work with in the Policy System.

If a component in the tree has a plus sign to its left, that means there are subcomponents nested below it. For example, if the component is a VLAN, then it has Extreme switches as subcomponents. The switches, in turn, have ports as subcomponents.

- ◆ Click on the plus sign to display the nested subcomponents.

The plus sign changes to a minus sign.

- ◆ Click on the minus sign to hide the subcomponent list.

THE STATUS/DETAIL INFORMATION PANEL

The right side panel displays information about the component selected in the tree on the left. For example, Figure 3-5 shows the Inventory Manager applet, with basic information about the devices known to the Enterprise Manager.

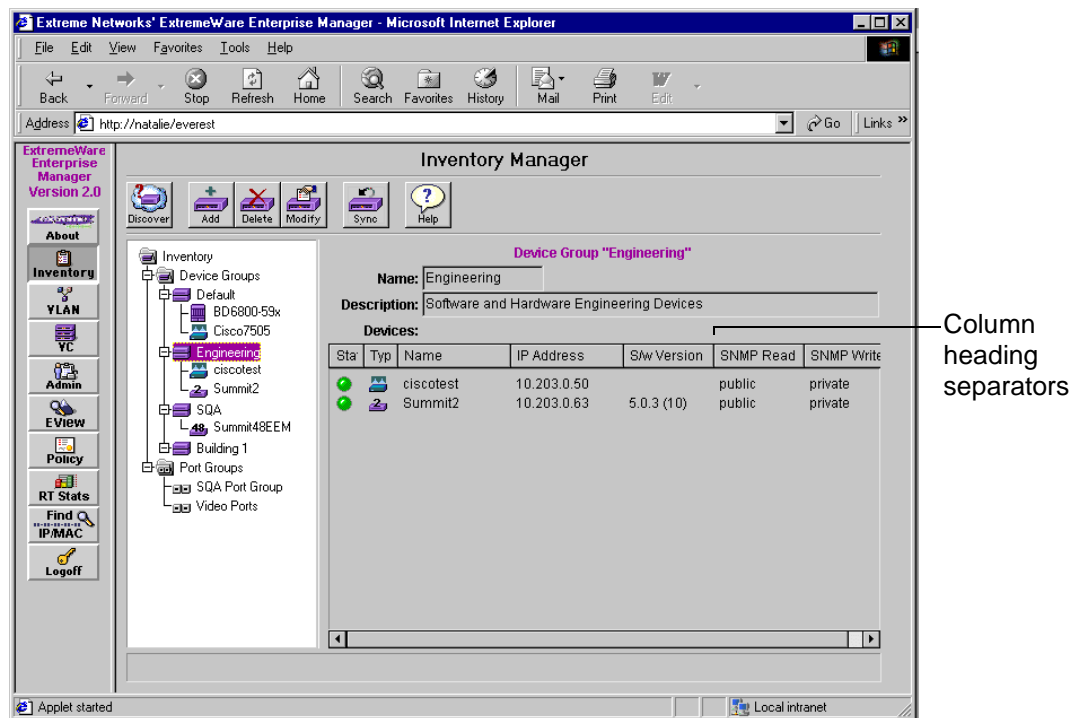


Figure 3-5: Inventory Manager applet

- Click on a component in the Component Tree to display information about that component.

In Figure 3-5, the selected component is the Default device group. The component status/detail panel displays summary status information about each device in this device group.

A red circle with the white "S" next to a device indicates that the device is not reachable through SNMP. This indicator may appear in any of the applets where a list of switches is displayed.

The buttons and frame contents change depending on which applet you are viewing, and also on the permissions associated with your user account.

MOVING THE COMPONENT TREE BOUNDARY

You can move the boundary between the Component Tree panel and the main applet panel by following these steps:

- 1 Place the cursor over the line separating the panels.
- 2 Click and hold the left mouse button to “grab” the panel separator.
- 3 Drag the separator until the panels are the desired widths.

RESIZING AND SORTING COLUMNS

In a wide columnar display such as shown in Figure 3-5, you can resize the widths of each column. To do this, follow these steps:

- 1 Place the cursor over the line separating the column you want to resize from the column to its right.
- 2 Click and hold the left mouse button to “grab” the column separator.
- 3 Drag the separator until the column is the desired width.

You can sort the rows of a columnar display according to the contents of any individual column.

- ◆ To sort the rows, click on the column heading you want to use as the sort criteria. Click once to sort in ascending order; click a second time to reverse the sort order.

APPLET FUNCTION BUTTONS

For all ExtremeWare Enterprise Manager applets (except the Inventory Manager and Admin applet), stand-alone buttons at the top of the applet frame provide access to the functions provided by the current applet. Each button invokes a pop-up dialog box for the function, as shown in Figure 3-6.

Note: *If you have Monitor access, some or all of the buttons in a given applet are not available to you. For example, in the VLAN Manager, a user with Monitor access can view information about the components in the Component Tree, but cannot Add, Delete, or Modify VLANs, or perform any port configurations.*

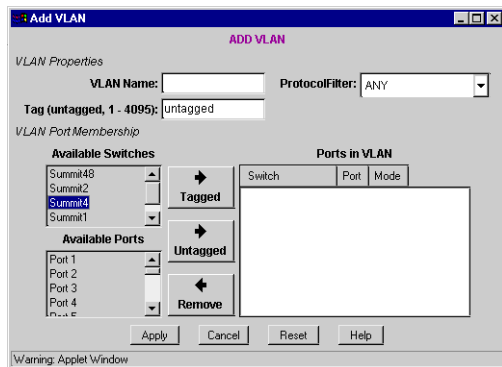


Figure 3-6: Pop-up dialog box for adding a VLAN in the VLAN Manager

A dialog box can contain the following types of fields:

- Text fields, such as the VLAN Name field in Figure 3-6. Enter text or numbers by clicking in the field and then typing.
To clear a value from a text field, highlight the value with the cursor and press the Del or Backspace key on the keyboard. You can also highlight the value and just type a new value over the old one.
- Drop-down menu fields, such as the Protocol Filter field in Figure 3-6. Click in the field to drop down a menu of choices, then click on your selection to enter the value into the field.
- List box fields, such as the Available Switches field in Figure 3-6. Click to highlight a value in the field. Click again to unselect a value.

If there are more entries in the list than can be displayed in the box, a scrollbar is provided at the right side of the field.

Some list boxes allow multiple selections. Simply click on multiple items to select them.

In addition, most dialog boxes contain a **Reset** button. This restores the dialog box to the state it was in when it was invoked, clearing any selections on the screen and resetting the data to the current information from the Enterprise Manager database.

4

Administering the ExtremeWare Enterprise Manager

This chapter describes how to use the Administration applet for the following:

- Adding ExtremeWare Enterprise Manager users.
- Setting and modifying user permissions for both the Enterprise Manager and ExtremeWare.
- Changing a user's password.
- Deleting users.
- Configuring the RADIUS server for user authentication.

OVERVIEW OF USER ADMINISTRATION

In order to log in to the ExtremeWare Enterprise Manager and use its management features, you must have a user name and password. You can also use the Enterprise Manager and its Remote Authentication Dial In User Service (RADIUS) server to configure access permissions for Extreme switches.

ENTERPRISE MANAGER ACCESS

The Enterprise Manager provides three levels of access to Enterprise Manager functions:

- Monitor—users who can view status information and statistics.
- Manager—users who can modify device parameters as well as view status information and statistics.

- Administrator—users who can create, modify and delete user accounts as well as perform all the functions of a user with Manager access.

The Enterprise Manager provides two default users, “admin” with Administrator access, and “user” with Monitor access. The two default users do not initially have passwords. All other user names must be added and enabled by an Administrator user.

Regardless of your access level, you can run the Administration applet and change your own password. Users with Administrator access can add and delete users and assign user access levels.

Note: *The ExtremeWare Enterprise Manager user accounts are separate from the Extreme switch user accounts. You can configure both through the Enterprise Manager, or you can have switch access independently of the Enterprise Manager.*

EXTREMEWARE ACCESS

Through the Enterprise Manager, two levels of access to Extreme switches can be enabled:

- User—users who can view device status information and statistics, but cannot modify any parameters.
- Administrator—users who can modify device parameters as well as view status information and statistics.

These permissions enable access to Extreme Networks switches through Telnet or ExtremeWare Vista. The use of the RADIUS server avoids the need to maintain user names, passwords, and access permissions in each switch, and instead centralizes the configuration in one location in the ExtremeWare Enterprise Manager.

THE RADIUS SERVER

ExtremeWare Enterprise Manager incorporates a basic RADIUS server for user authentication. RADIUS provides a standard way for the Enterprise Manager and Extreme switches to handle user authentication, permitting the unification of the Extreme CLI, ExtremeWare Vista, and Enterprise Manager authentication.

ExtremeWare versions 4.1 and later support the RADIUS server for authentication and can act as RADIUS clients.

STARTING THE ENTERPRISE MANAGER CLIENT FOR THE FIRST TIME

The two default users, admin and user, do not initially have passwords.

It is strongly recommended that you log in the first time with the user name admin, and immediately change the admin user password. You can then add other users with Manager, Monitor, or Administrator access.

To run the ExtremeWare Enterprise Manager client interface for the first time:

- 1 Launch your Web browser.
- 2 Enter the URL:

`http://<host>:<port>/`

In the URL, replace `<host>` with the name of the system where the ExtremeWare Enterprise Manager server is running. Replace `<port>` with the TCP port number that you assigned to the ExtremeWare Enterprise Manager Web Server during installation.

Note: *If you used the default web server port, 80, you do not need to include the port number.*

The Enterprise Manager Start-up page appears.

- 3 Launch the Enterprise Manager.

The Enterprise Manager Login page appears.

- 4 Type the user name **admin** in the User field.
- 5 Leave the Password field empty.
- 6 Click **Login**.

The About ExtremeWare Enterprise Manager window appears.

- 7 Click **Admin** to access the Administration functions of the Enterprise Manager.

The User Administration page appears, as shown in Figure 4-1. The only users are “admin” and “user.”

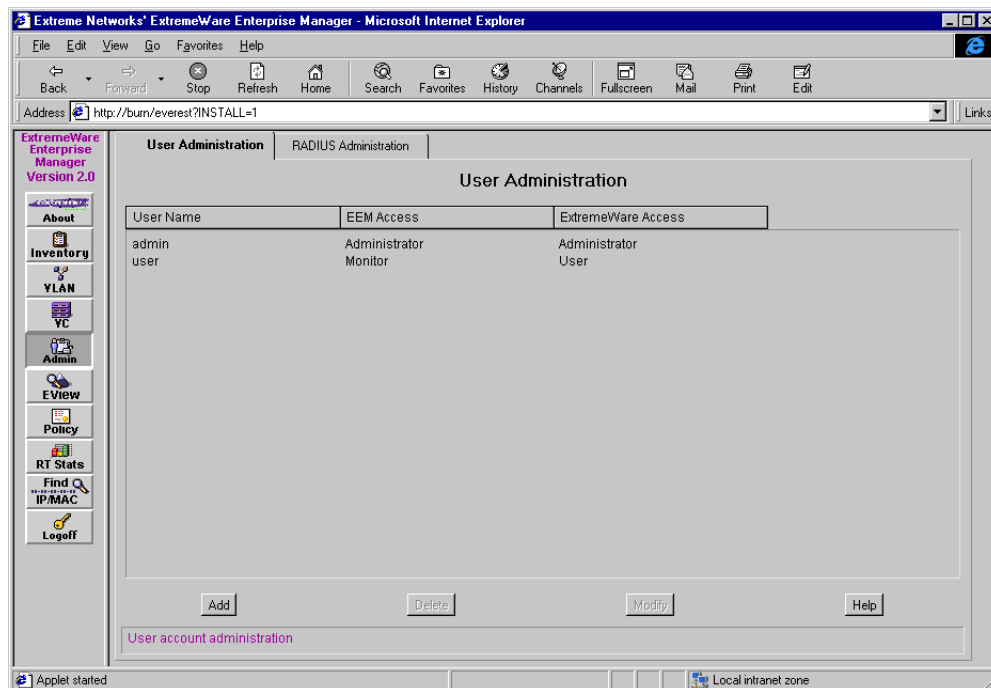


Figure 4-1: User Administration window

CHANGING THE ADMIN PASSWORD

To change the Admin password:

- 1 Click the tab at the top of the page to display the User Administration page, if necessary.
- 2 Select the user **admin** in the User list.
- 3 Click **Modify**.

The Edit User window appears, as shown in Figure 4-2.

Edit User

Name: admin

Password: [masked]

Verify Password: [masked]

EEM Account Access

- ☒ Administrator
- ☐ Manager
- ☐ Monitor
- ☐ Disabled

ExtremeWare Account Access

- ☒ Administrator
- ☐ User
- ☐ No Access

OK Cancel Help

Warning: Applet Window

Figure 4-2: Edit User window

- 4** Type a new password in the **Password** field.
- 5** Type the password again in the **Verify Password** field.
- 6** Click **OK**.

The new admin password is stored in the Enterprise Manager database. You cannot change the ExtremeWare Enterprise Manager access level for this user.

You can, however, change the ExtremeWare account access. The default for the ExtremeWare Enterprise Manager user “Admin” is Administrator. See the information under “Adding or Modifying User Accounts” for details on the ExtremeWare account access levels.

ADDING OR MODIFYING USER ACCOUNTS

To add users to the Enterprise Manager database, or to modify ExtremeWare Enterprise Manager user account access, follow these steps:

- 1 Login to the ExtremeWare Enterprise Manager as a user with Administrator access.
- 2 In the About ExtremeWare Enterprise Manager window, click **Admin** in the Navigation Toolbar.

The User Administration window appears.

- 3 Click the tab at the top of the page to display the User Administration page, if necessary.
- 4 To add a user, click **Add**. To change a user's access or password, select the user name and click **Modify**.

The New User window (or Edit User window) appears (Figure 4-3).

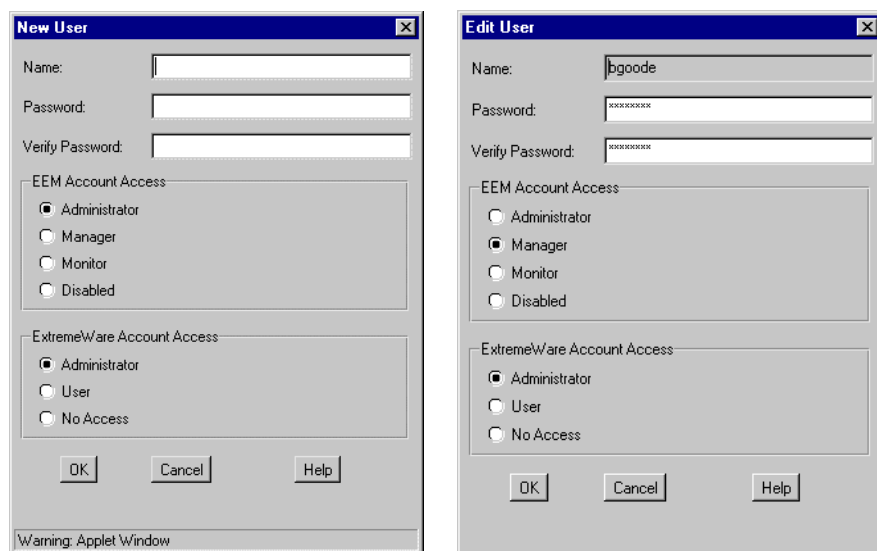


Figure 4-3: New User and Edit User windows

- 5 For a new user, type a user name into the **Name** field.
- 6 Type a new password into the **Password** field.
- 7 Type the password again into the **Verify Password** field.

8 Select the appropriate EEM Account Access level:

- **Administrator** access allows the user to add, edit and delete user accounts, as well as view status information and statistics and modify device parameters.
- **Manager** access allows the user to view status information and statistics and modify device parameters.
- **Monitor** access allows the user to view status information and statistics.
- **Disabled** provides no access privileges (the user will not be able to log in to the Enterprise Manager), but keeps the user account information in the Enterprise Manager database.

9 Select the appropriate ExtremeWare Account Access level:

- **Administrator** access allows the user to modify device parameters as well as view status information and statistics.
- **User** access allows the user to view device status information and statistics, but cannot modify any parameters.
- **No Access** provides no access privileges, but keeps the user account information in the Enterprise Manager database.

10 Click **OK**.

The new user information is stored in the Enterprise Manager database.

Note: *A change to a user account does not take effect until the next time the user logs in.*

DELETING USERS

To delete a user, follow these steps:

- 1** Log in to the ExtremeWare Enterprise Manager as a user with Administrator access.
- 2** At the About ExtremeWare Enterprise Manager window, click **Admin** in the Navigation Toolbar.

The User Administration page appears.

- 3** Select the user name you want to delete and click **Delete**.

Note: *You cannot delete the user name **admin**.*

A confirmation window appears.

4 Click **Yes**.

This removes all information about this user account from the Enterprise Manager database.

Note: *To remove all access privileges for a user without removing the user account from the Enterprise Manager database, use the Modify User function and change the Account Access to Disabled.*

CHANGING YOUR OWN USER PASSWORD

If you have Manager or Monitor access, you can change your own password at any time after you have logged in to the ExtremeWare Enterprise Manager. To do so, follow these steps:

1 Click **Admin** in the Navigation Toolbar.

The Change Password window appears, as shown in Figure 4-4.

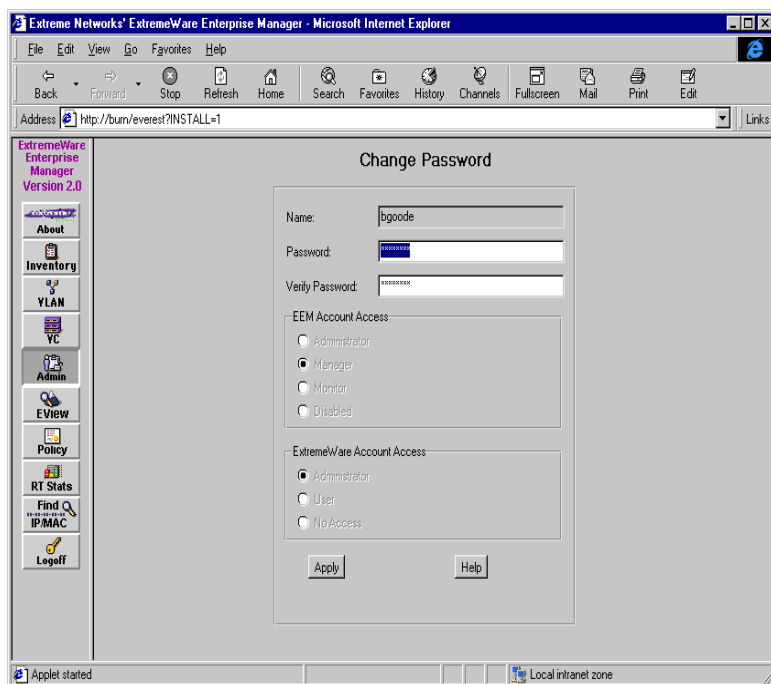


Figure 4-4: Change Password window

The window shows your user name, and your EEM and RADIUS Account Access levels as well as your password, but you cannot change them.

- 2 Type your new password in the **Password** field.
- 3 Type the password again in the **Verify Password** field.
- 4 Click **Apply**.

Your new password is stored in the Enterprise Manager database.

Note: *The change does not take effect until the next time you log in.*

RADIUS ADMINISTRATION

If you have Administrator access, you may enable or disable the RADIUS server, and change its port or the RADIUS secret.

To modify the RADIUS server settings, follow these steps:

- 1 From the User Administration page, click the **RADIUS Administration** tab.
The RADIUS Administration page appears, as shown in Figure 4-5.

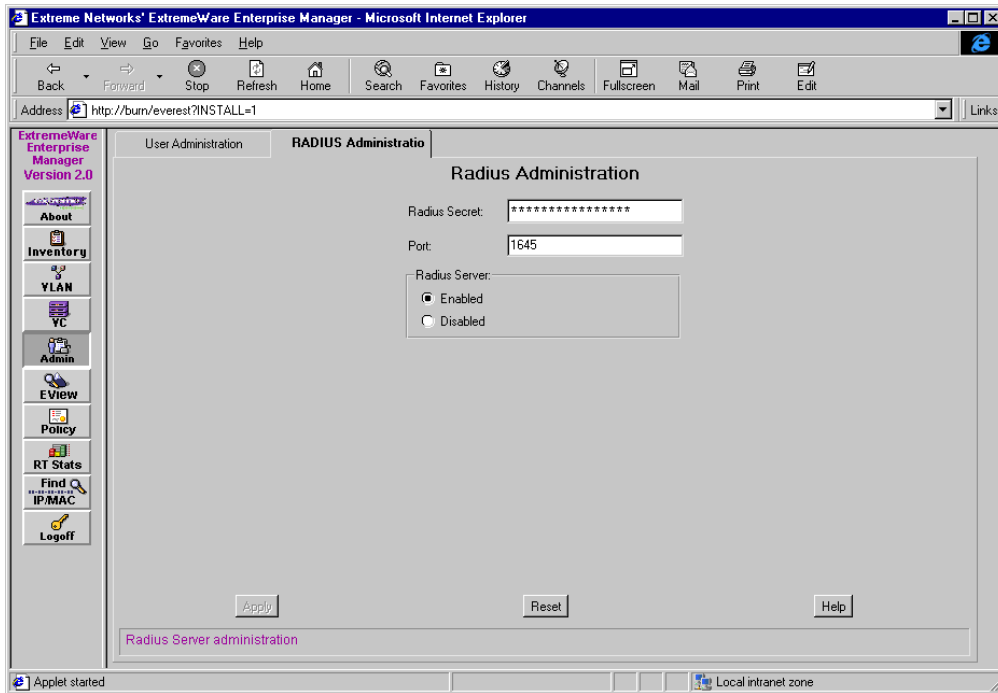


Figure 4-5: Radius Administration page

- 2 To change the RADIUS server's shared secret, simply type a new string in the Radius Secret field.

This string is basically a shared key by which the RADIUS server and its clients recognize each other, and which they use for secure transmission of user passwords.

Note: *If you change the secret in the RADIUS server, you must also change it in any of the RADIUS clients (Extreme switches) that use the RADIUS server for user authentication.*

- 3 To change the port, type a new port number in the Port field.

Note: *If you change the RADIUS server port, you must also change the port in any of the RADIUS clients (Extreme switches) that use the RADIUS server for user authentication.*

- 4 To enable or disable the RADIUS server, click the appropriate button.

Enabling the RADIUS server means that Extreme switches can act as RADIUS clients, authenticating users against the RADIUS server's database of users, as

administered through the Enterprise Manager. Thus, even if a user accesses the switch directly through Telnet or a browser, the RADIUS server will provide the authentication service.

Disabling the RADIUS server means that it will not be available for authenticating users. In this case, each Extreme switch must maintain its own list of users and access permissions, and users will need to remember a (possibly different) login and password for every switch.

5

Using the Inventory Manager

This chapter describes how to use the ExtremeWare Enterprise Manager Inventory Manager applet for:

- Viewing the ExtremeWare Enterprise Manager device inventory.
- Discovering network devices.
- Adding network devices to the ExtremeWare Enterprise Manager database.
- Modifying device contact parameters.
- Deleting a device from the ExtremeWare Enterprise Manager database.
- Updating device information in the database.

OVERVIEW OF THE ENTERPRISE MANAGER DEVICE INVENTORY

The Inventory Manager applet keeps a database of all the network devices managed by the ExtremeWare Enterprise Manager. ExtremeWare Enterprise Manager Version 2.0 can discover and manage Extreme switches, and several models of Cisco and Xedia devices.

The ExtremeWare Enterprise Manager 2.0 software provides an automatic discovery function. This feature can discover Extreme, Cisco, and Xedia devices by specific IP address or within a range of IP addresses.

You can also add network devices to the Enterprise Manager database manually, using the Inventory Manager Add function. Once a network device is known to the Enterprise

Manager database, you can assign it to a specific device group, and configure it using the VLAN Manager, Virtual Chassis Stack Manager, ExtremeView, or the Policy System.

Any Enterprise Manager user can view status information about the network devices currently known to Enterprise Manager. Users with Administrator or Manager access can run Discovery, and add devices to or delete devices from the list of managed devices in the database. These users can also explicitly refresh the information in the database related to the devices that the Enterprise Manager is managing.

DEVICE GROUPS

Devices in the ExtremeWare Enterprise Manager are organized into one or more *device groups*. A device group is a set of network devices that have something in common, and that can be managed as a group. For example, devices might be grouped by physical location (Building 1, Building 2, first floor, second floor) or by functional grouping (engineering, marketing, finance) or by any other criteria that makes sense within the managed network environment. An individual device may belong to one, and only one, device group. All devices become members of a device group when they are added to the Enterprise Manager database, either through Add Devices or as a part of the Discovery process. A device may then be moved to another device group as appropriate.

PORT GROUPS

Ports can also be organized into *port groups* to allow them to be manipulated as a unit. However, unlike devices, there is no default port group, and ports do not have to be members of a port group. Port groups are useful as policy objects, allowing a single policy definition to apply to multiple ports, even across devices.

GATHERING DEVICE STATUS INFORMATION

The ExtremeWare Enterprise Manager retrieves information about the devices it manages in several ways:

- The ExtremeWare Enterprise Manager uses SNMP polling for the IP addresses specified in a Discovery request to retrieve the status information needed by the various Enterprise Manager applets.
- When a switch is added manually to the Enterprise Manager database, the Enterprise Manager uses SNMP to retrieve status information needed by the various Enterprise Manager applets.

- Extreme switches send SmartTraps to the Enterprise Manager whenever a change occurs in a switch status variable that the Enterprise Manager has registered interest in. These include changes to operating variables as well as configuration changes made through other management entities such as the switch command line interface or ExtremeWare Vista.

These traps are based on a set of SmartTraps rules that the Inventory Manager creates on the switch when it is added to the switch inventory. The rules tell the switch what events or changes the Enterprise Manager wants to be notified about. The rules are created on the switch using SNMP. The Enterprise Manager also adds itself on the switch as a trap receiver. The switch uses the SmartTraps rules to determine what traps to send to the Enterprise Manager.

When the Enterprise Manager receives a trap from a switch, it then polls the switch for detailed status information.

- The Enterprise Manager polls every network device periodically (approximately every five minutes by default) to update basic switch status, a subset of the status and configuration information kept in the database.
- A user with Administrator or Manager access can use the **Sync** command from the Inventory Manager. **Sync** is a manual update of the regular data gathering mechanisms, for use when the users feels that the device configuration or status is not correctly reported in the Enterprise Manager applets. **Sync** causes the Enterprise Manager to poll the switch and update *all* configuration and status information. During a **Sync** operation the SmartTraps rules are also reset in case the user has accidentally deleted the trap receiver or any SmartTrap rules.

DISPLAYING THE NETWORK DEVICE INVENTORY

When you click the Inventory button in the Navigation Toolbar, the main Inventory Manager page is displayed as shown in Figure 5-1.

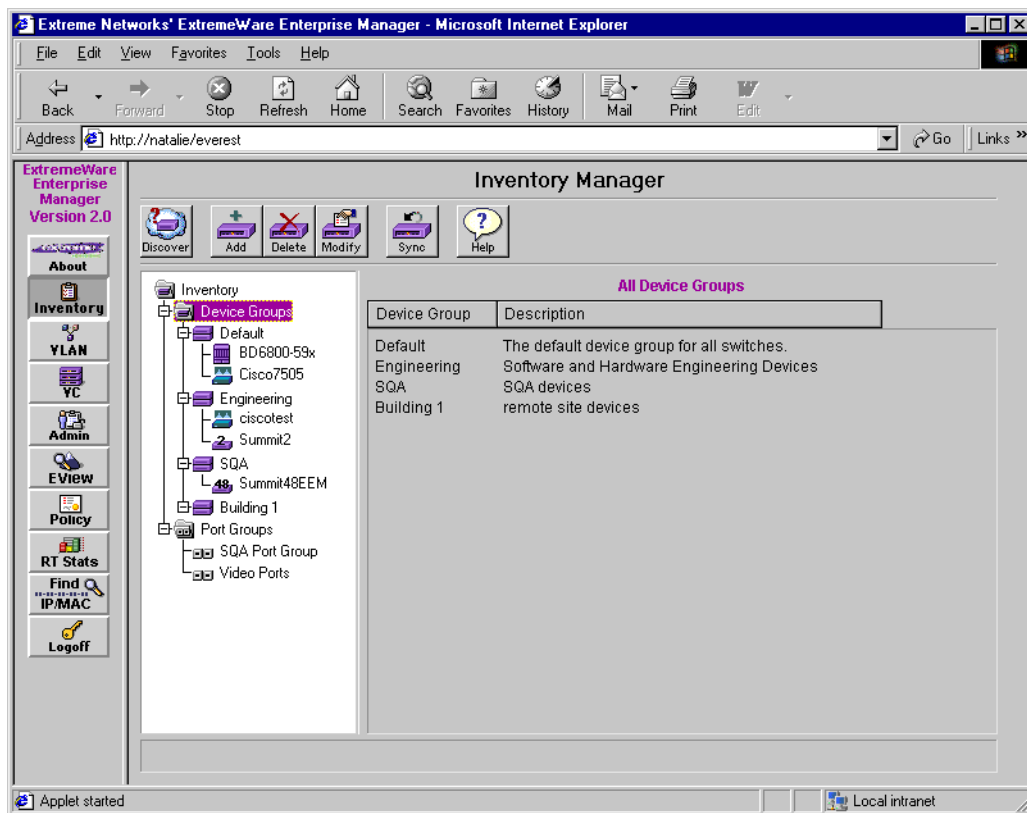


Figure 5-1: The Inventory Manager applet, main page

Note: You must add network devices to the database using Discovery or the Add Devices function in order to make them “known” to the ExtremeWare Enterprise Manager. Until this is done, no devices are displayed in the Inventory Manager.

The Device Groups currently defined in the Enterprise Manager are displayed in the Component Tree in the left panel.

The panel on the right shows the All Device Groups page, a list of the currently defined device groups with their descriptions.

The first time you run the ExtremeWare Enterprise Manager, there will be only one device group, **Default**. You cannot delete or change the name of the Default device group.

A red circle with the white “S” next to a device indicates that the device is not reachable through SNMP.

The buttons at the top of the page provide the following functions:

- **Discover** lets you find network devices by IP address or range of addresses.
- **Add** lets you add individual devices, device groups, and port groups to the database.
- **Delete** removes a device, device group, or port group from the database.
- **Modify** lets you change the members of a device group or port group, or update a device’s contact parameters in the database.
- **Sync** updates the Enterprise Manager database with current device configuration and status information.
- **Help** displays an on-line help page for the Inventory Manager.

VIEWING DEVICE STATUS INFORMATION

When you select a device group in the Component Tree, the panel on the right displays a summary status of the devices in the selected device group (see Figure 5-2).

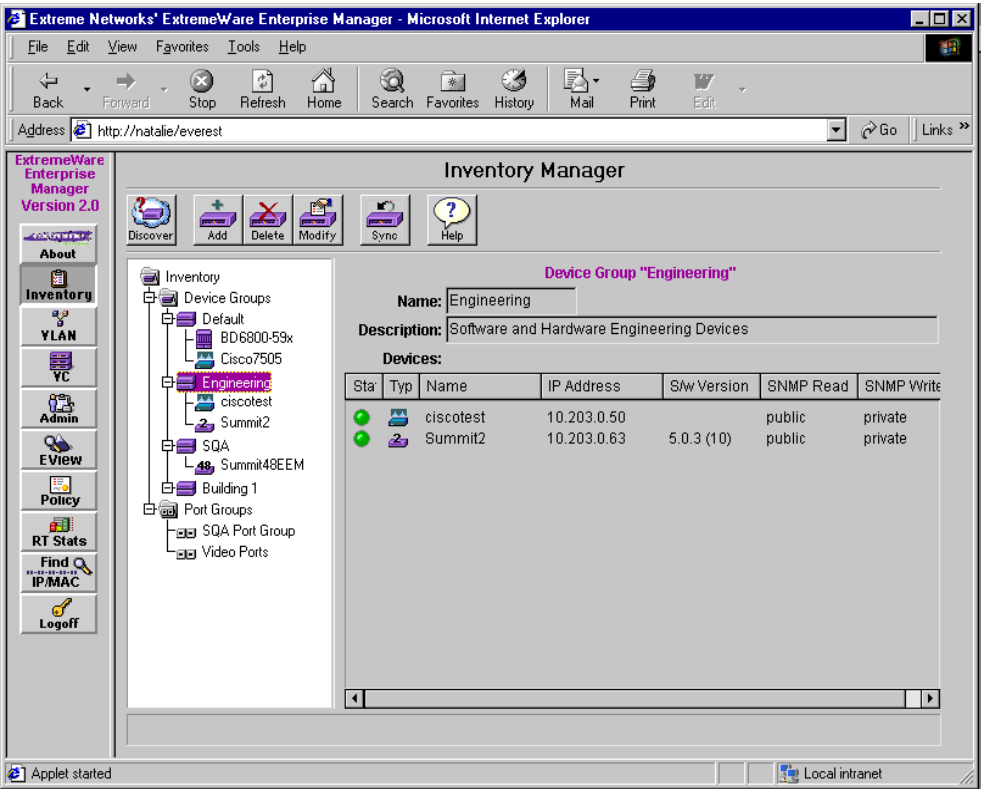


Figure 5-2: Inventory Manager device group summary status

- The status “lights” show the status of the device as detected by the ExtremeWare Enterprise Manager:

Table 5-1: Inventory Manager Device Status Indicators

Status Light	Device Status
Green	Device is up and OK
Yellow	Device is responding, but reports an error condition such as a fan or power supply failure, or excessive temperature
Red	Device is not responding to Enterprise Manager status queries. This may mean that the device is down, that it is unreachable on the network, or that the SNMP community strings have changed and the ExtremeWare Enterprise Manager can no longer contact the switch.

- The name and type of the device are detected by the ExtremeWare Enterprise Manager.
- The IP address and read/write community strings are also detected by the Enterprise Manager discovery, or are those entered into the ExtremeWare Enterprise Manager database manually if the switch was added using the Add command.

Select a switch in the Component Tree on the left to display detailed configuration and status information, as shown in Figure 5-3. This display shows additional information that the Enterprise Manager has gathered from the switch agent.

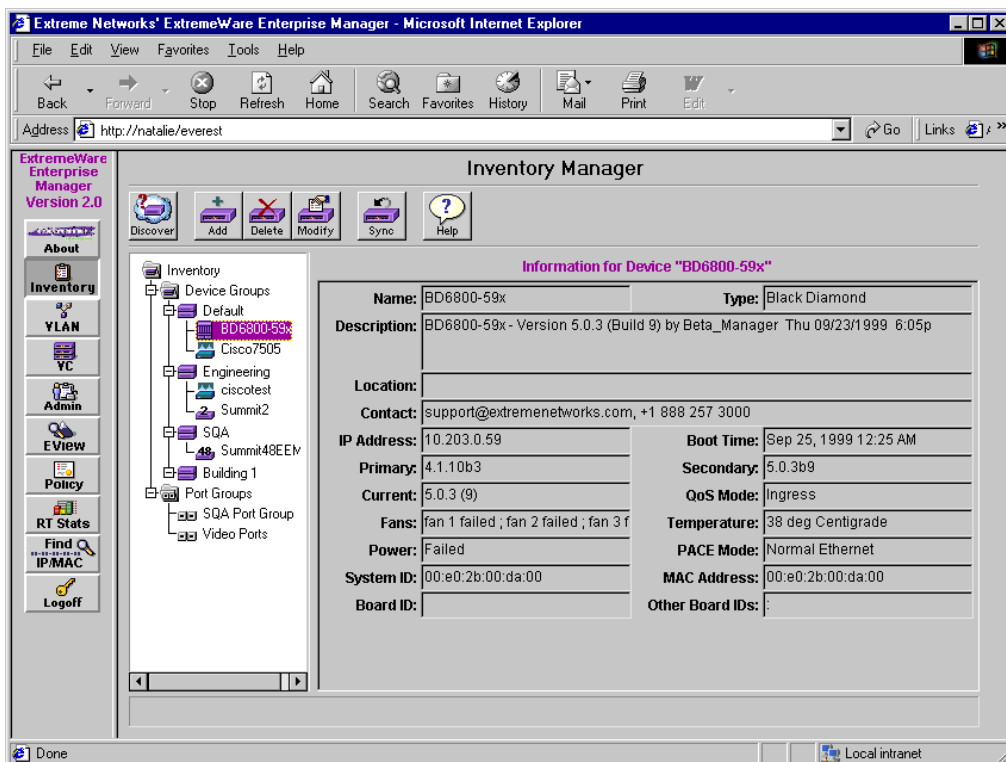


Figure 5-3: Inventory Manager device status information

The information displayed in Figure 5-3 is for an Extreme switch. The ExtremeWare software running in the switch provides comprehensive status information through the Extreme MIB. Figure 5-4 show the information displayed for a Cisco device—a subset of the information available for an Extreme device.

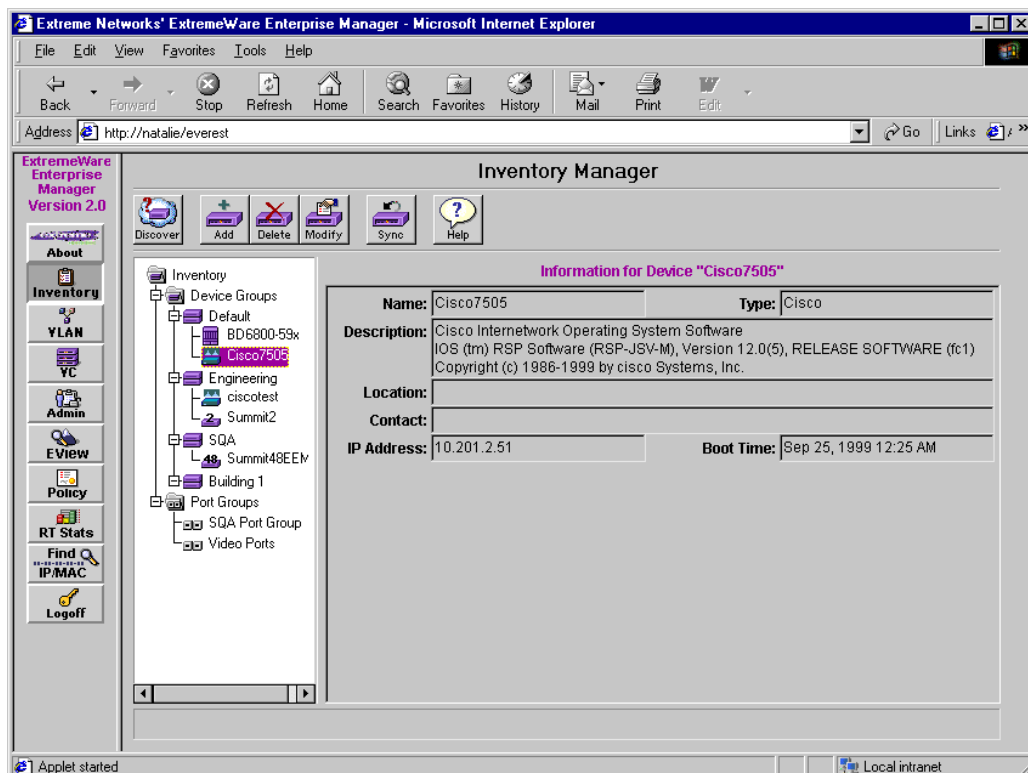


Figure 5-4: Inventory Manager information for a Cisco device

DISCOVERING NETWORK DEVICES

ExtremeWare Enterprise Manager 2.0 provides an automatic Discovery function that lets you discover network devices by IP address.

To discover network devices, do the following:

- 1 Click the **Discovery** button at the top of the Inventory Manager main window.
The Discover Devices window, as shown in Figure 5-5, is displayed.

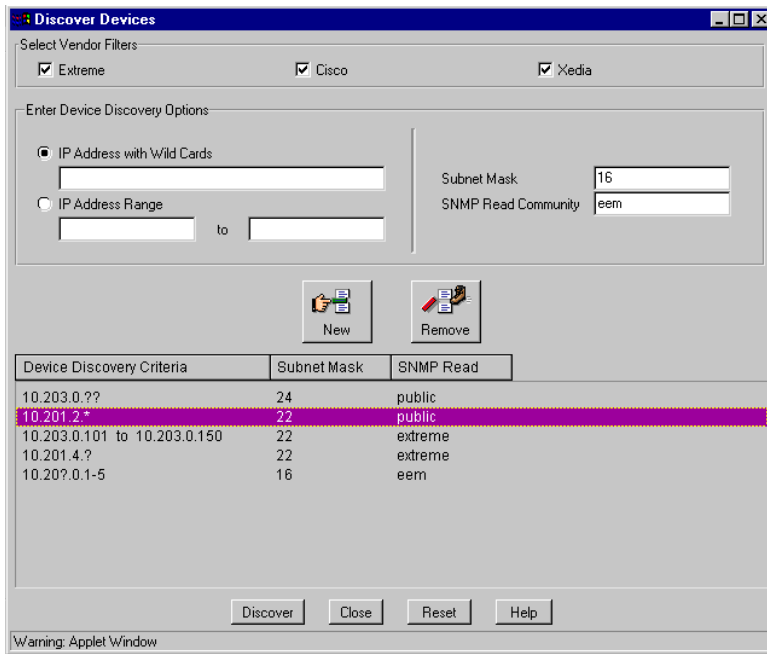


Figure 5-5: Inventory Manager Device Discovery set up window

- 2 Click the appropriate boxes to select the types of devices you want to include in the discovery. You can discover Extreme, Cisco, and Xedia devices.
- 3 Specify the device address range you want to discover. You may specify the range in one of two ways:

- As an **IP Address with Wildcards** (such as 10.203.10.* or 10.203.?.??).

Valid wildcard characters are *, ?, and - (dash):

- * acts as a wildcard for the entire octet (0-255).

- ? is a wildcard for a single digit (0-9).

- lets you specify a range for any octet. You can use this in more than one octet.

Note: You cannot combine the dash with another wildcard in the same octet.

You can also use the IP Address with Wildcards field to specify a single IP address.

Examples:

IP Address Specification	Addresses Generated
10.203.0.*	polls 10.203.0.0 through 10.203.0.255
10.203.?.??	polls 10.203.0.0 through 10.203.9.99
0.203.0.1? or 10.203.0.10-19	both specify the same range: 10.203.0.10 through 10.203.0.19
10.203.0-2.10-30	polls 10.203.0.10 through 10.203.0.30 10.203.1.10 through 10.203.1.30 10.203.2.10 through 10.203.2.30

— As an **IP address Range** (such as 10.203.10.20 to 10.203.10.45).

Note: *There certain IP addresses that are reserved. You should not include these addresses in your discovery.*

- *Class A networks 0 and 127 are reserved.*
- *Class D networks 224 - 239 are reserved for multicasting.*
- *All addresses above 239 are reserved.*
- *255 is reserved for broadcast datagrams for either the host or network portion of the IP address.*

In addition, certain host addresses may be interpreted as broadcast addresses, depending on the subnetting of your network.

The algorithm that processes IP addresses prior to initiating the discovery request eliminates IP addresses that contain 255's in the host portion. This decision is based on the IP address as well as the subnet mask.

- 4 Specify (or verify) the **Subnet Mask** size as appropriate. The value in the Subnet Mask field is the number of bits to be masked, starting from the high-order (left-hand) octet. The default subnet mask of 24 will mask the three high-order octets.
- 5 Specify (or verify) the **SNMP Read Community** string so that the Enterprise Manager will be able to retrieve information from any devices it discovers.
- 6 Click the **New** button to add the range into the Device Discovery Criteria list.
- 7 Repeat steps 3 through 6 to specify any additional device addresses or ranges for the discovery.

- 8 You can remove an address range from the Device Discovery Criteria list at any time before you initiate the discovery by selecting the range and clicking the **Remove** button.

You can remove all address ranges using the **Reset** button at the bottom of the page.

- 9 Click the **Discover** button at the bottom of the window to initiate the discovery.

If the discovery criteria results in a discovery of more than 1500 devices, a dialog appears informing you of the number of items in your search request, and asking you for confirmation. Click **Yes** to proceed or **No** to refine the discovery criteria.

Note: *If a discovery request is too large, your browser may not have sufficient memory resources available to handle it. It is recommended that you break a large discovery task into multiple separate tasks.*

A Discovery Results window is displayed as soon as the discovery process begins, as shown in Figure 5-6. The panel at the bottom of the window shows the progress of the discovery and displays status messages for each device it finds as it works through the set of IP addresses you have specified.

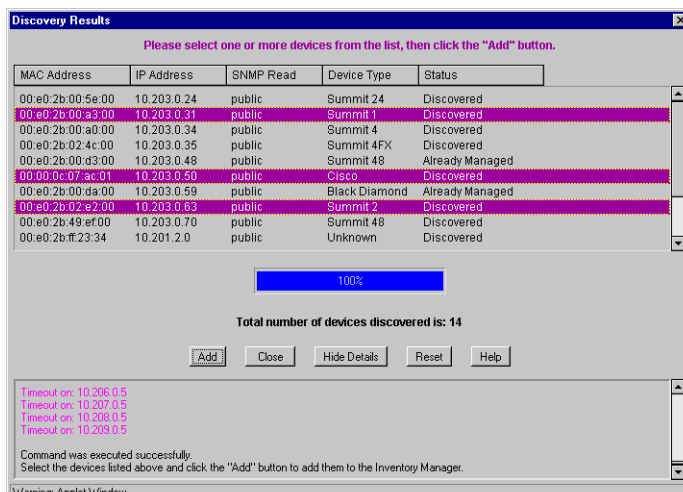


Figure 5-6: Results of a discovery, with details visible

Click the **Hide Details** button at the bottom of this window to remove the detail display. Click **View Details** to re-display the discovery details.

When the discovery has completed, the set of discovered devices is listed in the top panel of the Discovery Results window.

Note: These devices are NOT automatically entered into the Enterprise Manager database. You must explicitly select and add devices to the database.

- 10 To add devices to the ExtremeWare Enterprise Manager database, select individual devices or a range of devices in the Results list, and click the **Add** button at the bottom of the window.

Note: If you select multiple devices, make sure the devices you select are similarly configured. As part of the Add process, you will be asked for a **single** password that will apply to all the selected devices. If the password is specified incorrectly for any of these devices, the add will fail for those devices.

- 11 A window (Figure 5-7) pops up where you must set additional device options such as a write community string, the device group to which the devices should be added, and a default device login and password. If there are Cisco devices among the set being added, you must also enter a Cisco enable password.

Enter or make changes to any of these fields. These options will apply to the entire set of devices you are adding.

Note: Make sure the device passwords are correct for the selected devices. If you are adding multiple devices in one operation, make sure the passwords you specify are correct for all those devices. A device cannot be added if the password is not correct.

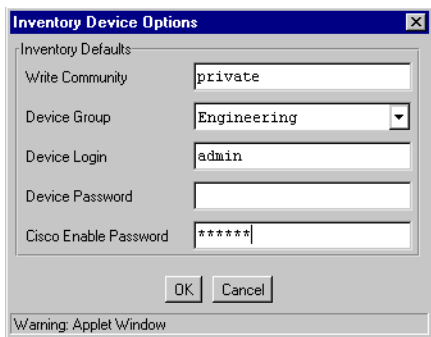


Figure 5-7: Setting default device options for discovered devices

- 12 Click **OK** to proceed with the Add process.

A message window (shown in Figure 5-8) pops up to show you the progress of the Add command.

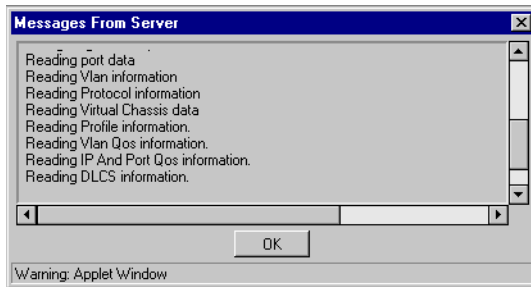


Figure 5-8: Message window showing Add device progress

Warning: *If you close the Discovery Results window without adding devices, the results for any devices not already in the ExtremeWare Enterprise Manager database are lost. You will need to perform a discovery again to regenerate information on those devices.*

After the Add has finished, the Discovery Results window is re-displayed. You can select more devices and specify a different set of Inventory Device Options, and add those devices to the Inventory Manager.

ADDING DEVICES, DEVICE GROUPS AND PORT GROUPS

Users with Administrator or Manager access can add devices to the ExtremeWare Enterprise Manager database, and create Device Groups and Port Groups. If you have Monitor access only, you are not able to use this function.

ADDING A DEVICE

- 1 Click the **Add** button at the top of the Inventory Manager main window. Select the appropriate tab to display the Add Device window, as shown in Figure 5-9.

Add Devices, Device Groups, and Port Groups

Device | Device Groups | Port Groups

Device Information

IP Address: 10.0.5.3 | SNMP Read: cisco | SNMP Write: switch

Device Login: admin | Device Password: ***** | Device Group: Engineering

Cisco Enable Password: *****

New Remove

IP Address	SNMP Read	SNMP Write	Device Login	Device Group
10.203.0.41	summit	aspen	admin	Default
10.201.0.132	summit	aspen	admin	Engineering
10.0.5.3	cisco	switch	admin	Engineering

Add Close Reset Help

Warning: Applet Window

Figure 5-9: Add Device window in the Inventory Manager

- 2 Enter the device IP address, community strings, device login and password into the appropriate fields. These are the parameters that the Enterprise Manager uses to access the switch.

You may also enter a DNS-resolvable host name in place of the Switch IP address.

- 3 Select the device group to which this device should belong. It can belong to only one device group. **Default** is the default group for managed devices.
- 4 To clear the contents of the fields and reset them to their default values, click **Reset**.
- 5 To add the new device into the database, click **Add**.

When you click **Add**, the Inventory Manager adds the devices to the database. It makes a set of SNMP requests to retrieve data that is needed from the devices by the Enterprise Manager applets. If the device is an Extreme switch, it also creates a set of

SmartTraps rules that tell the switch what status and configuration changes are of interest to the Enterprise Manager.

CREATING A DEVICE GROUP

Device groups are sets of managed network devices that have something in common, and that can be managed as a group. For example, devices might be grouped by physical location, (Building 1, Building 2, first floor, second floor) by department (engineering, marketing, finance) or by any other criteria that makes sense within the managed network environment.

Every device belongs to one, and only one, device group. All devices become members of a device group when they are added to the Enterprise Manager database, either through Add Devices or as a part of the Discovery process. A device may then be moved to another device group as appropriate.

To create a new device group, follow these steps:

- 1** Click the **Add** button at the top of the Inventory Manager main window.

Select the appropriate tab to display the Device Groups window, as shown in Figure 5-10.

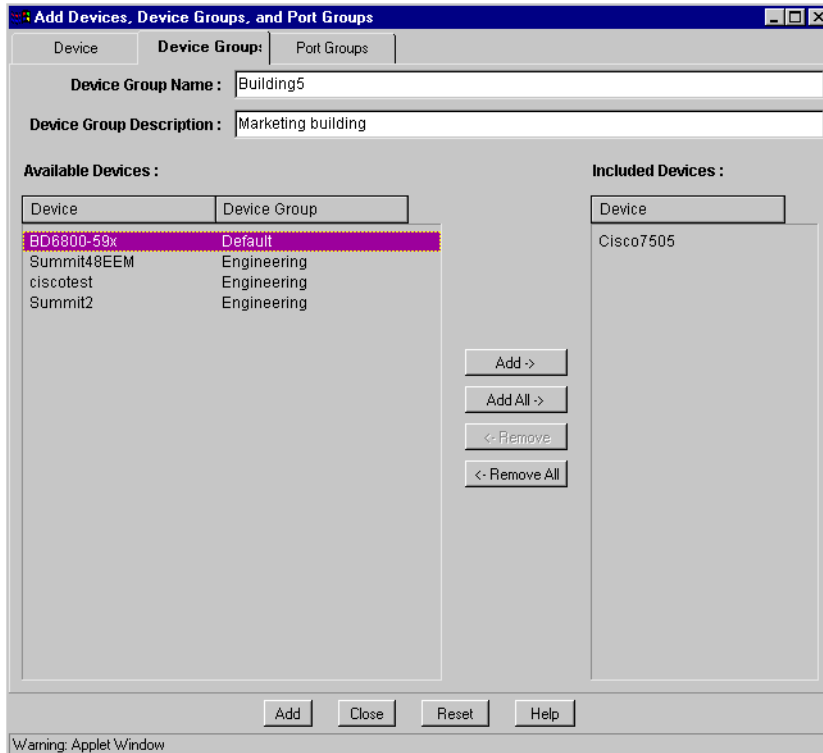


Figure 5-10: Add Device Group window in the Inventory Manager

- 2 Type a name for the device group into the **Device Group Name** field, and a description (optional) into the **Device Group Description** field.
- 3 To add a device to the selected device group, select the device in the Available Devices list and click **Add ->**. To add all devices in the Available Devices list, click **Add All ->**.
- 4 To remove a device from the device group, select the device in the Included Devices list, and click **<- Remove**. The device will be moved from the selected device group to the Default device group. To return all devices in the Included Devices list to the Default device group, click **<- Remove All**.
- 5 Repeat steps 3 and 4 until you have included all the devices that should be members of this device group.
- 6 To add the list of newly created device groups to the database, click the **Add** button at the bottom of the window.

CREATING A PORT GROUP

A port group is a set of ports that have something in common, and can be manipulated as a unit. A port group may contain ports from many different switches. Unlike device groups, there is no default port group, and ports do not need to be members of a group. However, they can belong to only one port group at a time. Port groups are useful as policy objects, allowing a single policy definition to apply to multiple ports, even across devices.

To create a port group, follow these steps:

- 1 Click the **Add** button at the top of the Inventory Manager main window.

Select the appropriate tab to display the Port Groups window, as shown in Figure 5-11.

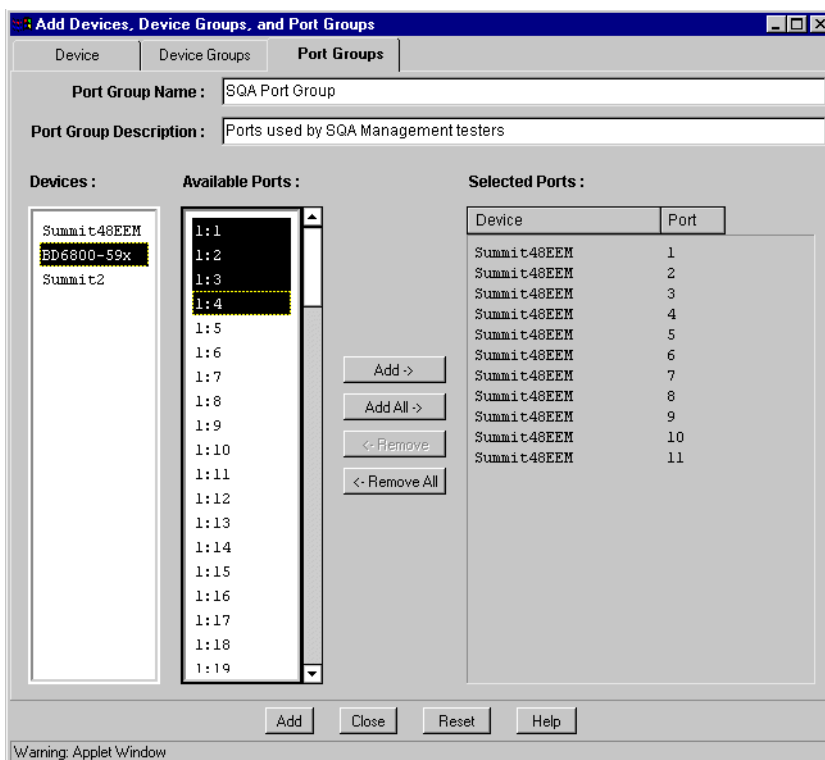


Figure 5-11: Add Port Group window in the Inventory Manager

- 2 Type a name for the port group into the **Port Group Name** field, and a description (optional) into the **Description** field.
- 3 Select a device from the **Devices** list. This displays a list of ports on the switch that are available to be included in the port group.
- 4 Select one or more ports from the **Available Ports** list. Click the **Add ->** button in the middle of the screen to add these ports to the **Selected Ports** list. Click the **Add All ->** button to add all ports from the device to the Selected Ports list.
- 5 To remove a set of ports from the Selected Ports list, select the ports and use the **<- Remove** button. Use **<- Remove All** to clear the Selected Ports list.
- 6 Repeat steps 3 through 5 until you have included all the ports that should be members of this port group.
- 7 To add the new port group to the database, click the **Add** button at the bottom of the window.

MODIFYING DEVICES, DEVICE GROUPS AND PORT GROUPS

You can use the Modify function to modify the access parameters for an individual device, or to add and delete members of a device group or port group. Users with Administrator or Manager access can modify device contact information, device groups and port groups.

If you have Monitor access only, you can not use this function.

MODIFYING A DEVICE

To modify the contact information for a managed device in the database, do the following:

- 1 Click the **Modify** button at the top of the Inventory Manager main page.
Select the appropriate tab to display the Modify Device window, as shown in Figure 5-12.

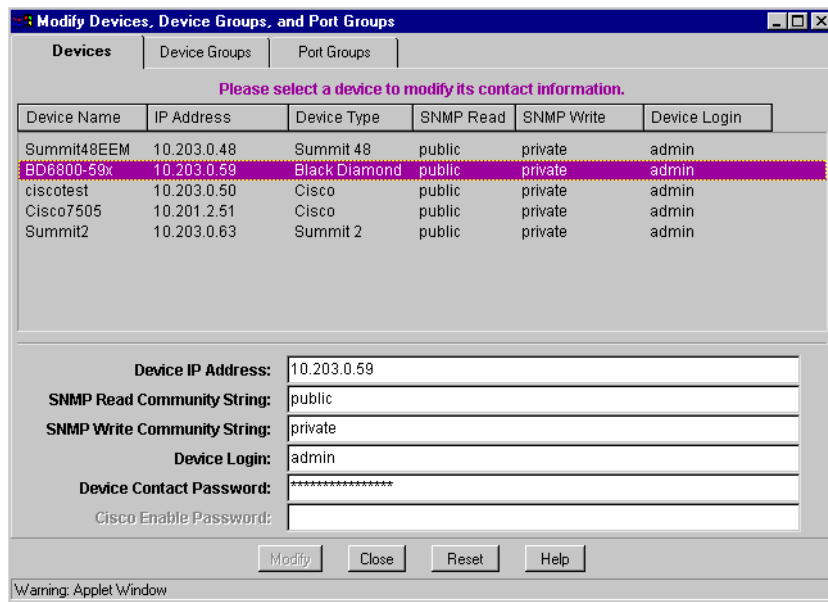


Figure 5-12: Devices tab of the Modify Devices, Device Groups, and Port Groups window.

- 2 Select the device for which you want to change contact information.
- 3 Enter the changed information in the appropriate fields.

The Device Login and Device Password are the login and password needed in order to Telnet to the device or to use ExtremeWare Vista

- 4 Click **Reset** to change the fields back to their original values.
- 5 Click **Modify** to add the changed information to the ExtremeWare Enterprise Manager database.
- 6 Click **Cancel** to cancel the Modify process.

MODIFYING A DEVICE GROUP

To add or remove devices in a device group, do the following:

- 1 Click the **Modify** button at the top of the Inventory Manager main page.
Select the appropriate tab to display the Modify Device Group window, as shown in Figure 5-13.

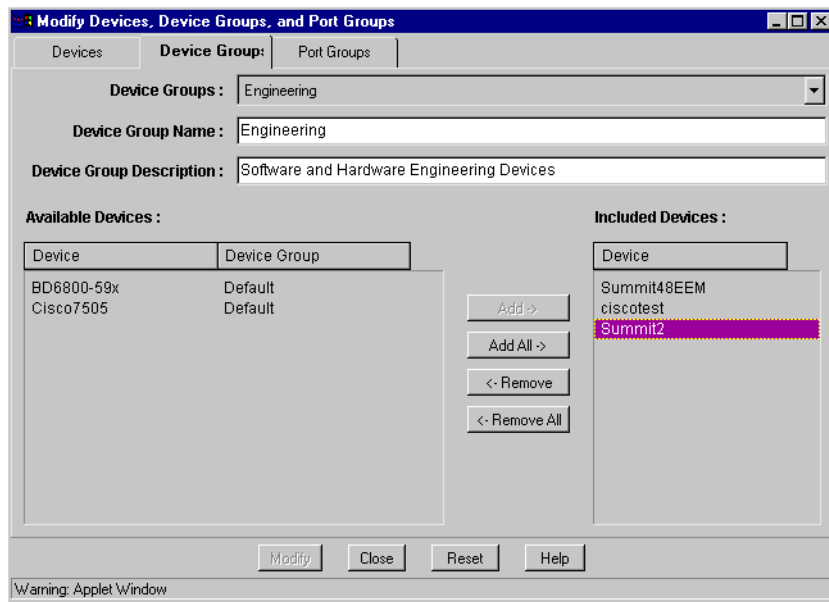


Figure 5-13: Device Groups tab of the Modify Devices, Device Groups, and Port Groups window.

- 2 Select the device group you want to modify. The Included Devices list displays the devices that are currently members of this group. The Available Devices list displays the other devices known to the Enterprise Manager, and their current device group membership.
- 3 To change the name or description of the group, type the new text into the **Device Group Name** and **Description** fields.
- 4 To add a device to the selected device group, select the device in the Available Devices list and click **Add ->**. To add all devices in the Available Devices list, click **Add All ->**.
- 5 To remove a device from the device group, select the device in the Included Devices list, and click **<- Remove**. The device will be moved from the selected device group to the Default device group. To return all devices in the Included Devices list to the Default device group, click **<- Remove All**.
- 6 Repeat steps 4 and 5 until you have included all the devices that should be members of this device group.
- 7 To replace the modified device group in the database, click the **Modify** button at the bottom of the window.

Moving a device from one device group to another requires two steps. First, remove it from its current device group (returning it to the Default group). Then select the new device group, and move the device from the Default device group to the new group.

MODIFYING A PORT GROUP

To add or remove ports from a port group, or to rename the group or change its description, do the following:

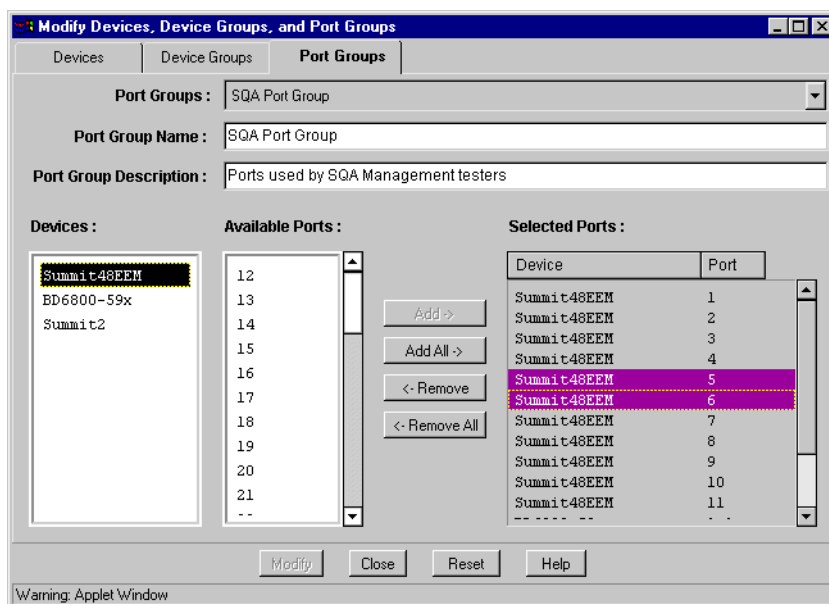


Figure 5-14: Port Groups tab of the Modify Devices, Device Groups, and Port Groups window.

- 1 Select the port group you want to modify from the Port Groups pull-down list.
- 2 To change the name or description, type the new text into the **Port Group Name** field and the **Description** field.
- 3 To remove a set of ports from the Selected Ports list, select the ports and use the **<- Remove** button. Use **<- Remove All** to clear the Selected Ports list.
- 4 To add ports to a group, first select a device from the **Devices** list. This displays a list of ports on the switch that are available to be included in the port group.

- 5 Select one or more ports from the **Available Ports** list. Click the **Add ->** button in the middle of the screen to add these ports to the **Selected Ports** list. Click the **Add All ->** button to add all ports in the Available Ports list to the Selected Ports list.
- 6 Repeat steps 3 through 5 until you have included all the ports that should be members of this port group.
- 7 To replace the modified port group in the database, click the **Modify** button at the bottom of the window.

DELETING DEVICES, DEVICE GROUPS, AND PORT GROUPS FROM THE DATABASE

Users with Administrator or Manager access can delete devices, device groups and port groups from the ExtremeWare Enterprise Manager database. If you have Monitor access only, you can not access this function.

DELETING A DEVICE

To delete a device from the Enterprise Manager database, follow these steps:

- 1 Click the **Delete** button at the top of the Inventory Manager main page.
Select the appropriate tab to display the Delete Devices window (see Figure 5-15).

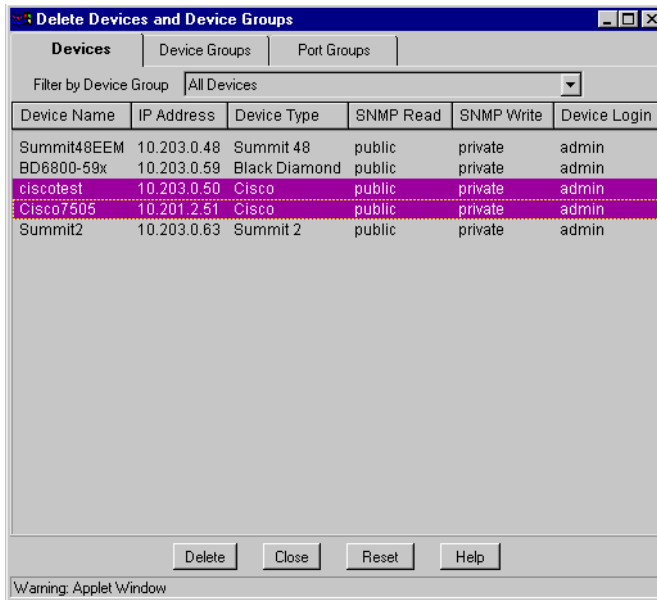


Figure 5-15: Devices tab of the Delete Devices and Device Groups window.

- 2 To select a device from a specific device group, select the device group from the pull-down list in the **Filter by Device Group** field. Select **All** to view the list of all devices from all device groups.
- 3 Select one or more devices in the Devices list, and click **Delete**.
- 4 Click **OK** to confirm that you want to delete the device information from the database.

Deleting a device removes the information about the device from the Enterprise Manager database. This means that the device can no longer be monitored and managed from the ExtremeWare Enterprise Manager application. If the device is an Extreme switch, deleting it removes any SmartTraps rules, both from the database and the switch change table. It also removes all information about VLANs, QoS Policy, and Virtual Chassis connections associated with this switch from the Enterprise Manager database.

Note: *Deleting a device from the Enterprise Manager has no effect on the configuration of the device itself.*

DELETING A DEVICE GROUP

To delete a device group from the Enterprise Manager database, follow these steps:

- 1 Click the **Delete** button at the top of the Inventory Manager main page.

Select the appropriate tab to display the Delete Device Groups window (see Figure 5-16).

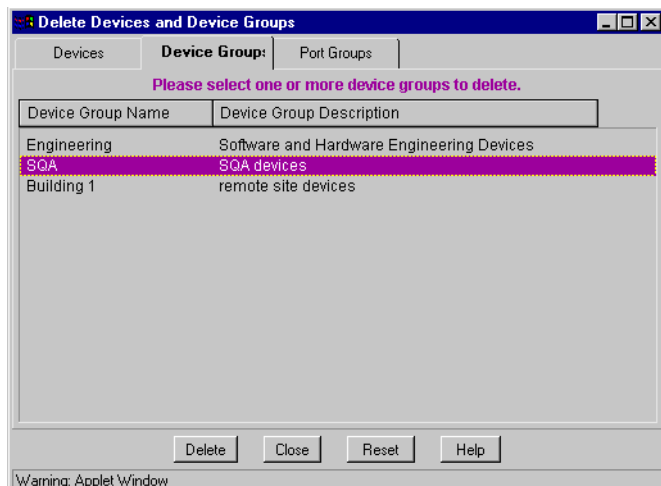


Figure 5-16: Device Groups tab of the Delete Devices, Device Groups, and Port Groups window.

- 2 Select one or more device groups in the Device Groups list, and click **Delete**.
- 3 Click **OK** to confirm that you want to delete the device group information from the database.

DELETING A PORT GROUP

To delete a port group from the Enterprise Manager database, follow these steps:

- 1 Click the **Delete** button at the top of the Inventory Manager main page.

Select the appropriate tab to display the Delete Port Groups window (see Figure 5-17).

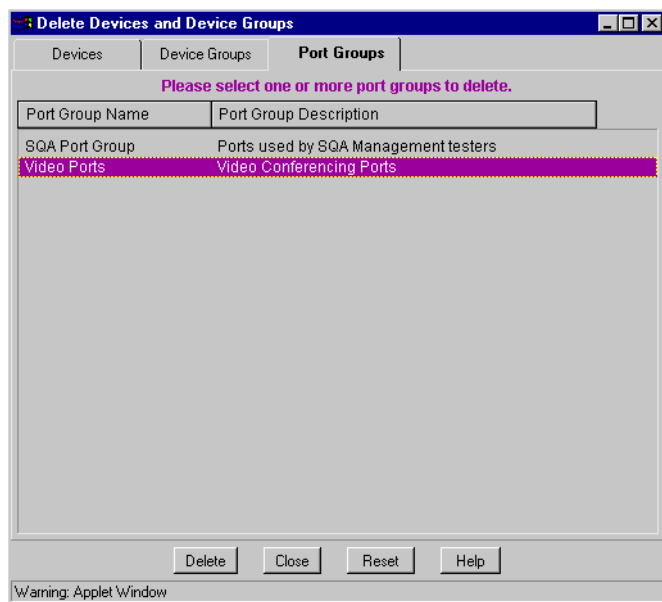


Figure 5-17: Port Groups tab of the Delete Devices, Device Groups, and Port Groups window.

- 2 Select one or more port groups in the Port Groups list, and click **Delete**.
- 3 Click **OK** to confirm that you want to delete the port group information from the database.

UPDATING DEVICE INFORMATION

Occasionally, you may want to update the configuration and status information for one or more devices in the ExtremeWare Enterprise Manager database. The **Sync** operation is a manual update you can use if you feel that the device configuration is not correctly represented in the Enterprise Manager applets. It updates all information for a selected set of devices, except for the contact information.

If you have Administrator or Manager access to the Enterprise Manager, you can perform a **Sync**. If you have Monitor access only, you can not use this function.

To refresh the configuration and status information, follow these steps:

- 1 Click **Sync** at the top of the Inventory Manager page.

The Synchronize Devices dialog, as shown in Figure 5-18, is displayed, listing the devices in the Enterprise Manager database.

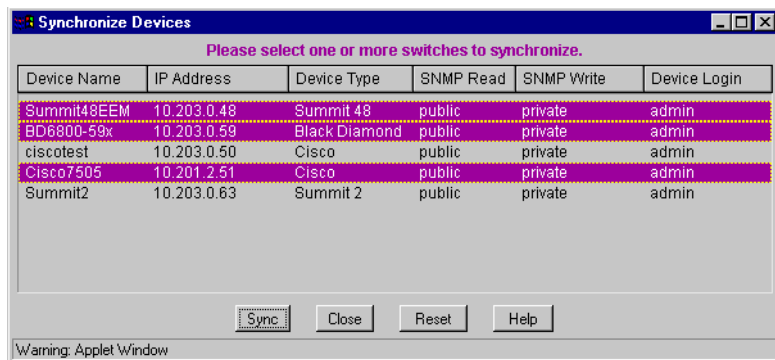


Figure 5-18: Synchronize Devices dialog

- 2 Select one or more devices in the Device list.
- 3 Click **Sync** to initiate the synchronization process.

The Inventory Manager uses SNMP to retrieve configuration and status information from each selected switch, and updates the database with that information.

- 4 Click **Reset** at any time prior to initiating the Sync to deselect all you device selections and start over.
- 5 The Sync function displays a dialog box with status or error information. Click **OK** to continue.

6

Using ExtremeView

This chapter describes how to use ExtremeView for:

- Viewing Extreme switch status
- Viewing and setting Extreme device configuration information using the ExtremeWare Vista graphical user interface
- Viewing Extreme device statistics
- Configuring Extreme devices using Telnet and the ExtremeWare Command Line Interface (CLI)
- Configuring Cisco devices using interactiveTelnet

OVERVIEW OF THE EXTREMEVIEW APPLICATION

The ExtremeView applet displays information about the status of Extreme switches (Summit and Black Diamond switches). Any Enterprise Manager user can view status information about these network devices known to the Enterprise Manager. Users with Administrator or Manager access can view and modify configuration information for those switches using either the ExtremeWare Vista graphical user interface, or using Telnet and the ExtremeWare Command Line Interface (CLI). You can also use the interactive Telnet capability to view and modify configuration information for Cisco devices.

ExtremeWare Vista is device management software running in a Summit or Black Diamond switch. It allows you to access the switch over a TCP/IP network using a standard Web browser, and provides a set of commands for configuring and monitoring the Summit or Black Diamond switch.

Note: You must have a user account on the Extreme switch in order to run ExtremeWare Vista on the switch. A user account on a switch is separate from your Enterprise Manager user account.

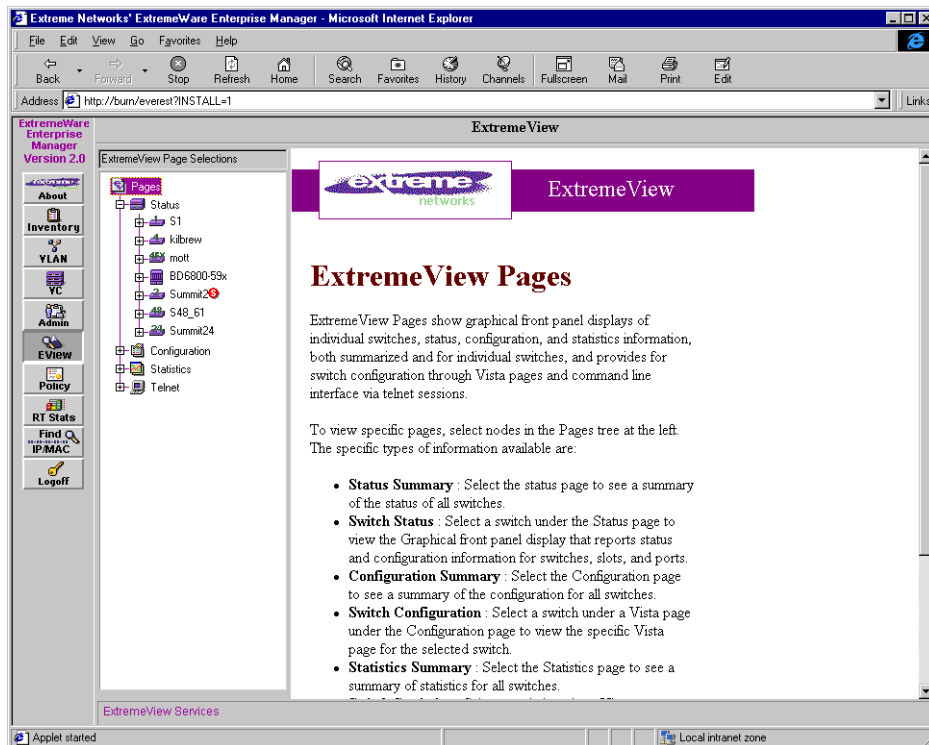


Figure 6-1: The ExtremeView applet, main page

- **Status** displays status information for the Extreme switches known to the ExtremeWare Enterprise Manager. You can view summary status for all network devices as well as status and configuration information for individual devices through a front panel view as well as a table of information.
- **Configuration** displays configuration information based on the configuration categories in ExtremeWare Vista. You can view summary configuration information as well as configuration information for individual switches, organized by ExtremeWare Vista configuration categories.
- **Statistics** displays monitoring results, also based on ExtremeWare Vista statistics monitoring categories. You can view summary statistics for active and inactive port counters, or statistics for individual switches.

- **Telnet** starts a macro application that allows the scripting and playback of CLI commands to a selection of Extreme switches. The applet performs a Telnet to the switch, logs into the switch, and performs the scripted commands. You can also use this applet to run an interactive Telnet session to an individual switch.

VIEWING SWITCH STATUS INFORMATION

Select **Status** in the Component Tree to display a summary status of the Extreme switches known to the Enterprise Manager (see Figure 6-2).

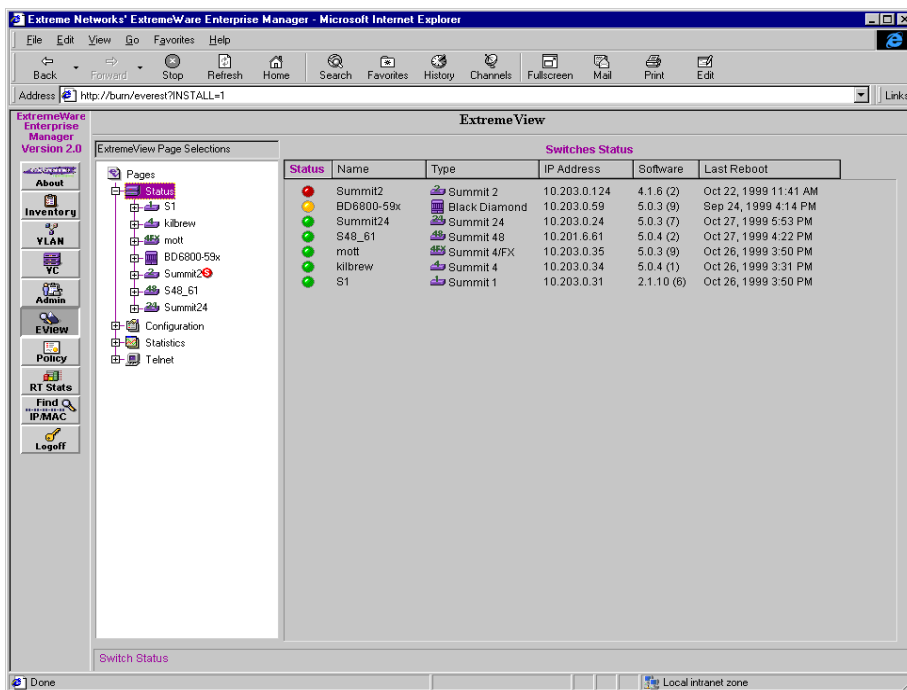


Figure 6-2: The ExtremeView applet, Status summary

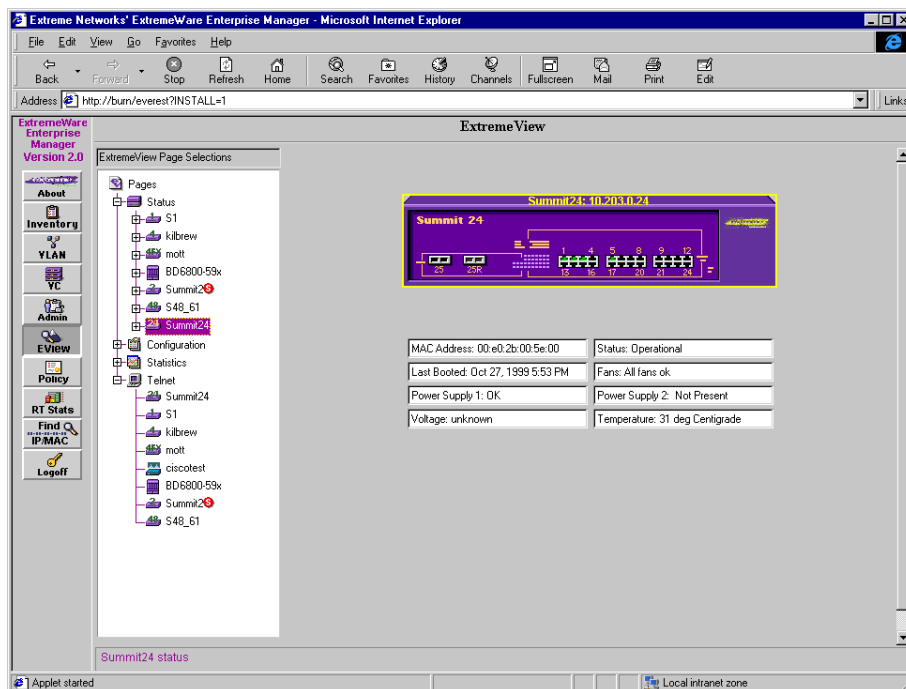
- The status “lights” show the status of the device as detected by the ExtremeWare Enterprise Manager.

Table 6-1: ExtremeView Switch Status Indicators

Status Light	/Switch Status
Green	Switch is up and OK
Yellow	Switch is responding, but reports an error condition such as a fan or power supply failure, or excessive temperature
Red	Switch is not responding to Enterprise Manager status queries. This may mean that the switch is down, that it is unreachable on the network, or that the SNMP community strings have changed and the ExtremeWare Enterprise Manager can no longer contact the switch.

- The name, type of switch, IP address, the ExtremeWare software version, and the last reboot time are retrieved from the switch by the ExtremeWare Enterprise Manager.

Select a switch in the Component Tree on the left to display detailed configuration and status information, as shown in Figure 6-3. This display shows additional information that the Enterprise Manager has gathered from the switch agent.

**Figure 6-3:** The ExtremeView applet, switch status

This view shows an active graphical display of the switch front panel, as well as a table of status information.

You can view the status of individual ports, as shown in Figure 6-4, in two ways:

- By selecting the port with the cursor in the switch diagram.
- By displaying the list of ports in the Component Tree, and selecting the port.

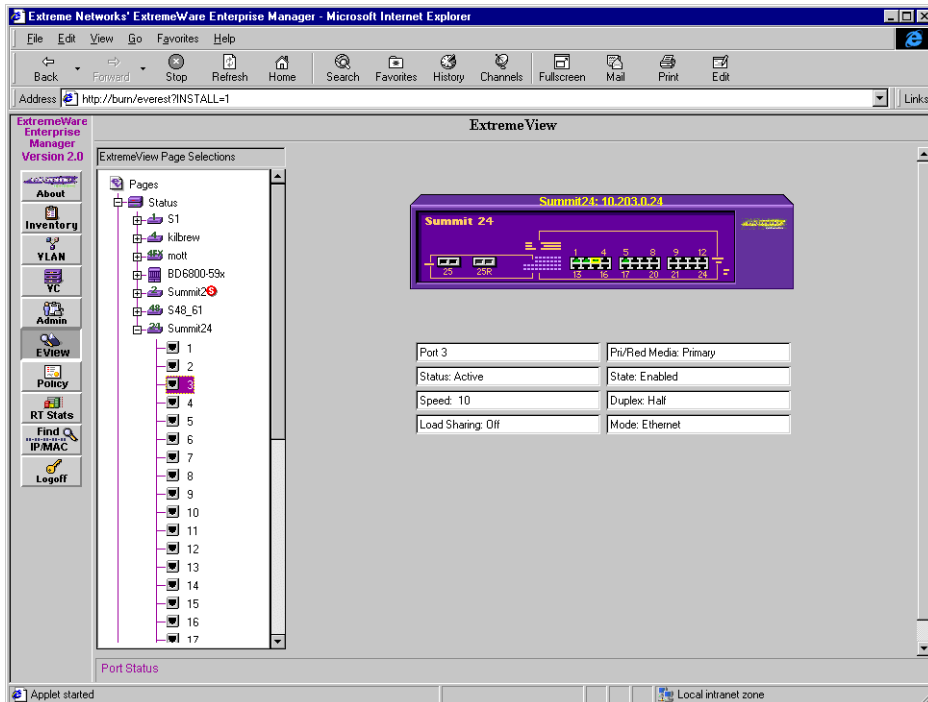


Figure 6-4: The ExtremeView applet, port status

You can remove the text fields by clicking anywhere on the page outside the switch image.

VIEWING SWITCH CONFIGURATION INFORMATION

Select **Configuration** in the Component Tree to display a configuration summary for the Extreme switches known to the Enterprise Manager (see Figure 6-5).

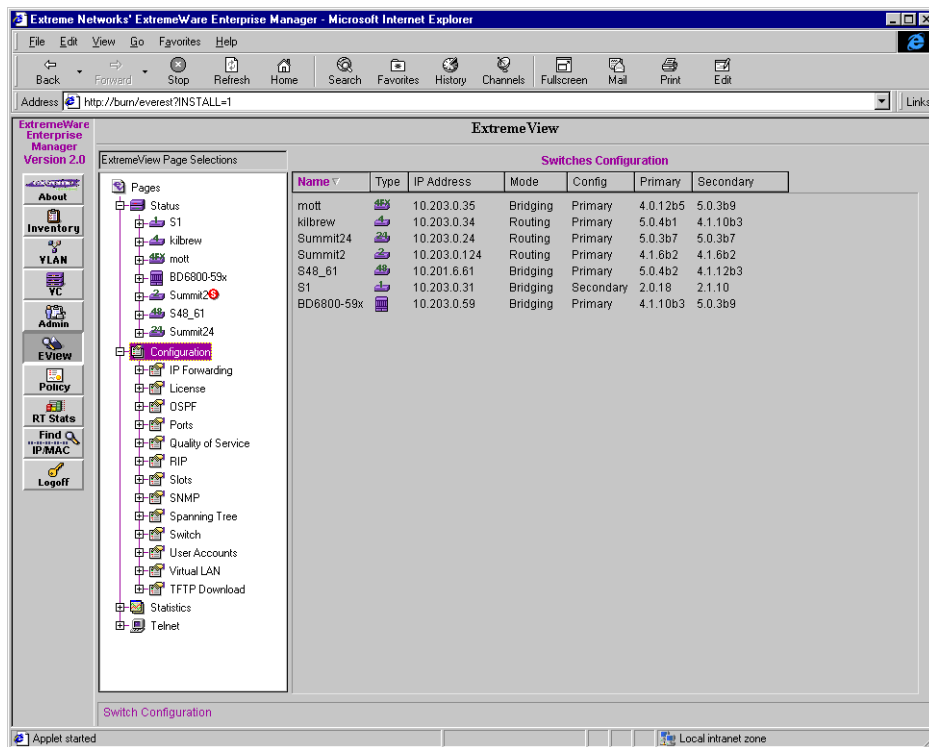


Figure 6-5: The ExtremeView applet, Configuration summary

The sub-components under Configuration in the Component Tree are the categories of configuration information that are available through this applet. These correspond to pages from the ExtremeWare Vista application running on the switch.

Select one of these categories to display a list of switches, and select a switch to view the configuration settings for that switch in the category you've chosen.

As shown in Figure 6-6, this displays the current switch configuration, and provides an interface through which you can change the configuration.

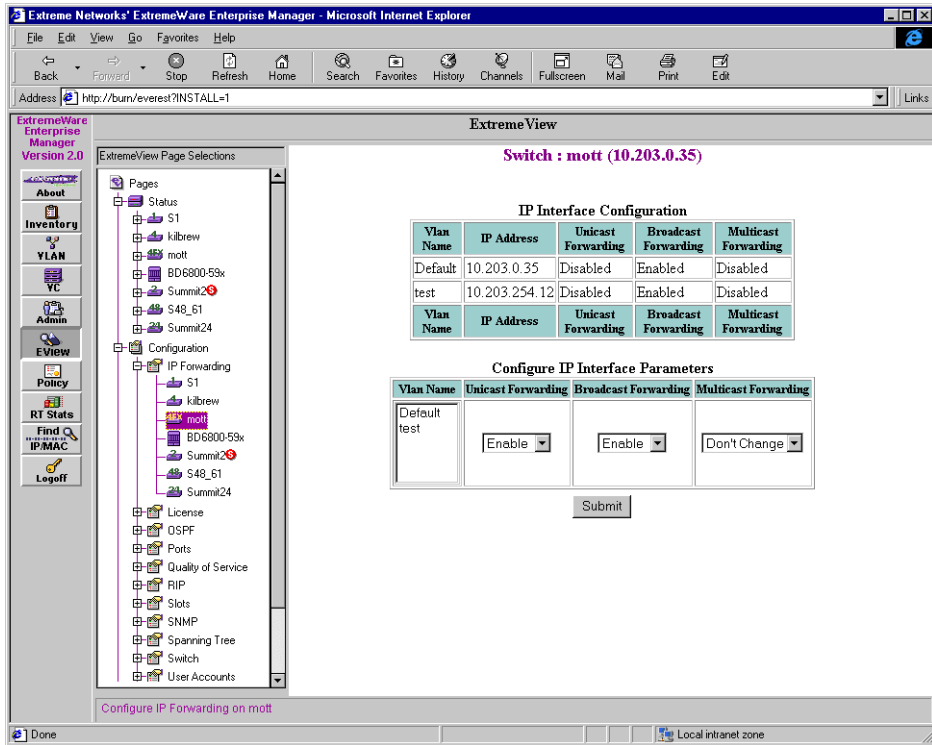


Figure 6-6: The ExtremeView applet, Configuration details

When you have made the necessary configuration changes, click **Submit** to send these to the switch for implementation.

VIEWING SWITCH STATISTICS

Select **Statistics** in the Component Tree to display summary statistics for the Extreme switches known to the Enterprise Manager (see Figure 6-7).

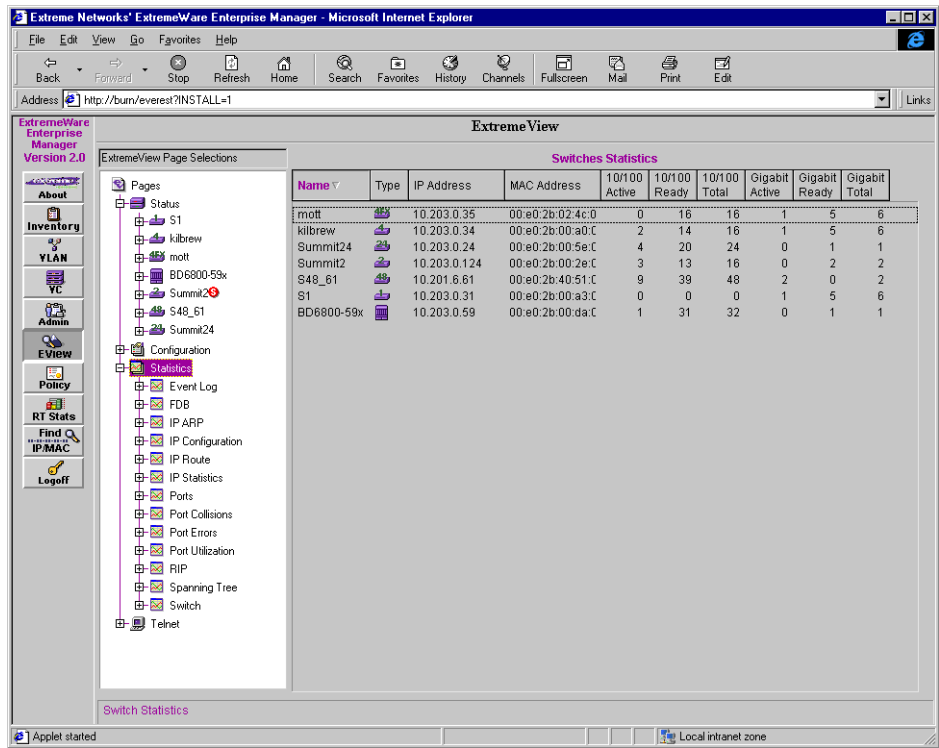


Figure 6-7: The ExtremeView applet, Statistics summary

The sub-components under Statistics in the Component Tree are the categories of statistical information that are available through this applet. These correspond to pages of information from the ExtremeWare Vista application running on the switch.

- Select one of these categories to display a list of switches, and select a switch to view the configuration settings for that switch in the category you've chosen.

This displays the selected set of statistics for the selected switch. For some types of statistics, as for those shown in Figure 6-8, you may be able to view the data in different ways through the use of View Options.

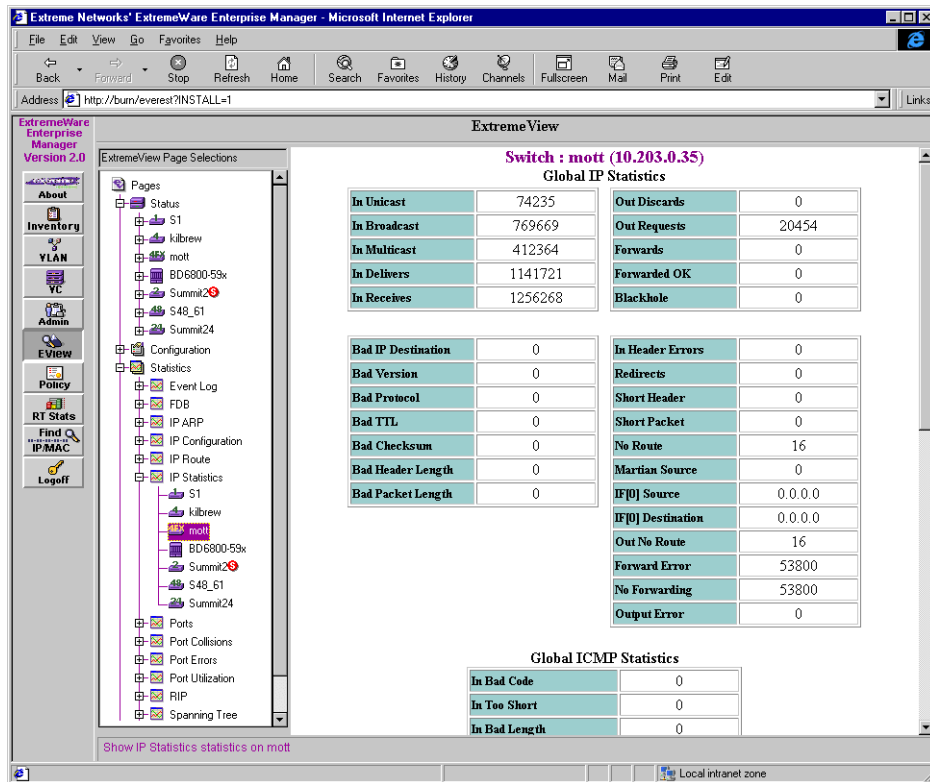


Figure 6-8: The ExtremeView applet, Statistics details

USING TELNET WITH EXTREME SWITCHES

The Telnet applet allows the scripting and playback of groups of CLI commands (macros) to a selection of Extreme switches. You can also use this applet to run an interactive telnet session on an individual switch, including third-party switches.

Select **Telnet** in the Component Tree to display a list of the telnet sessions for the Extreme switches in the Enterprise Manager database (see Figure 6-9).

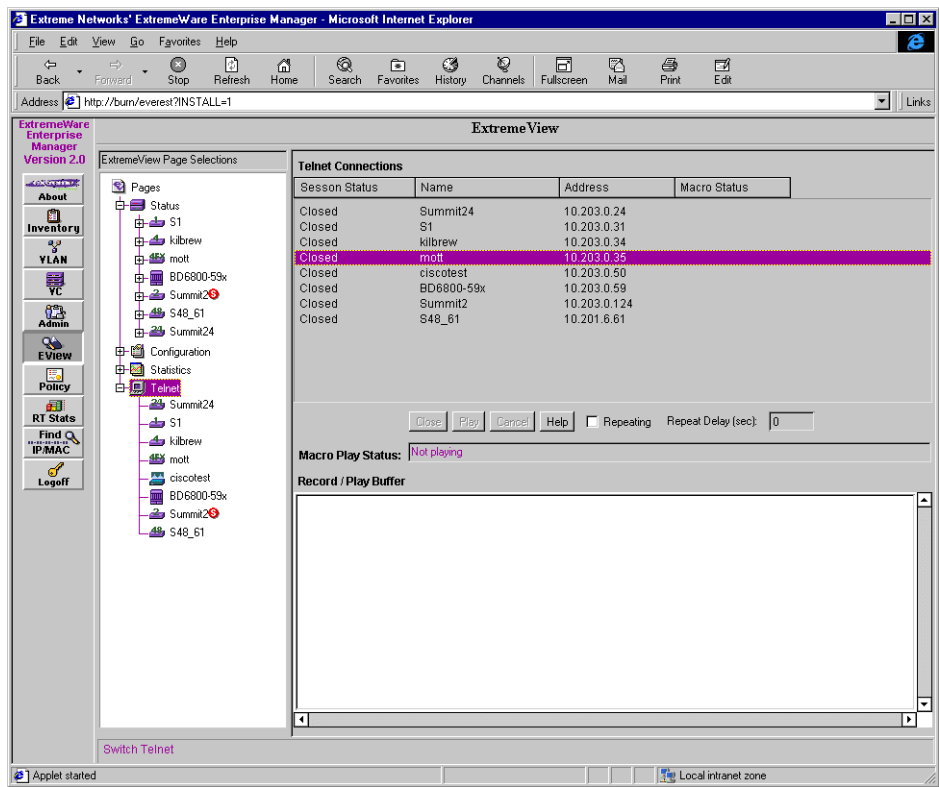


Figure 6-9: The ExtremeView applet, Telnet interface

The Telnet Connections lists indicates which switches have open Telnet connections, and the status of any macros that have run or are being run on the switch.

Switches with open Telnet connections are also shown in bold in the list of switches under the Telnet component in the Component Tree.

Note: If a switch displayed in the Component Tree has an “S” in a red circle along with the name, that means that the switch is not responding to SNMP requests. However, the switch may still respond to HTTP and Telnet requests.

RUNNING EXTREMEWARE COMMAND MACROS

The lower half of the Telnet page contains the macro Record/Play buffer. You can enter a series of ExtremeWare commands into this buffer, which will form a script that can be played to the set of switches you select in the Telnet Connections list.

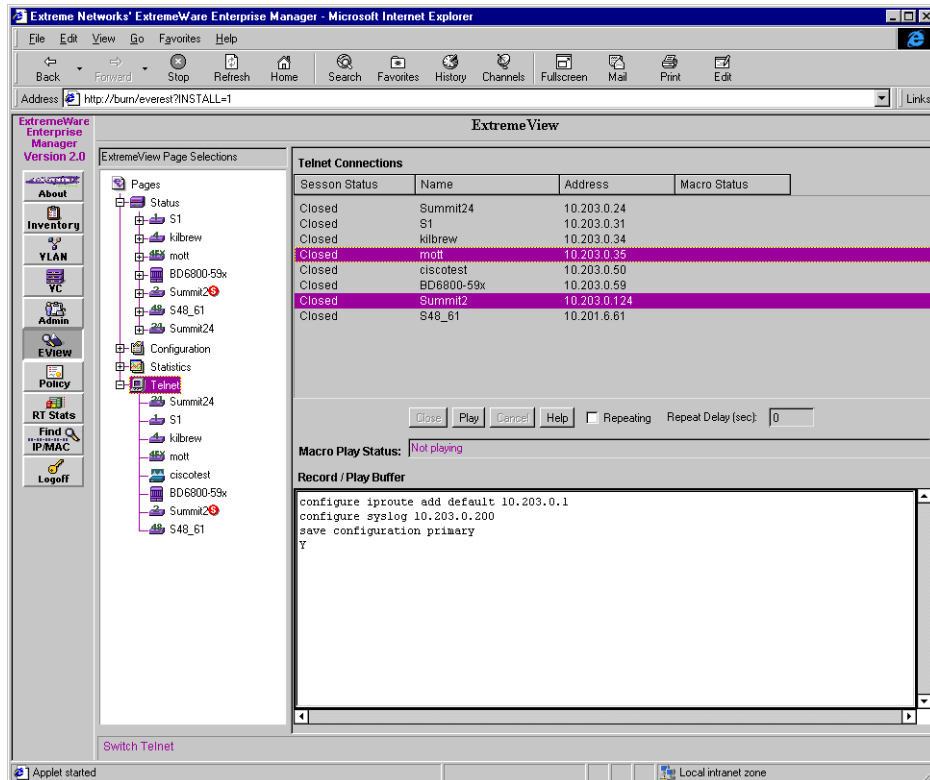


Figure 6-10: The ExtremeView applet, record and play buffer

To create a macro for playback to a set of Extreme switches, follow these steps:

- 1 Select the set of switches in the Telnet Connections list where you want your command macro to run. The switches do not need to have a telnet session already open—the macro play function will open a connection and log into the switch.
- 2 Enter a series of ExtremeWare commands into the Record/Play buffer.

There are four variables you can use in an ExtremeWare CLI command that will be expanded when the target switch is contacted. These are:

Table 6-2: ExtremeView Macro Variables

Variable	Definition
<NAME>	The name of the switch
<DATE>	The current date of the EEM server
<TIME>	The current time of the EEM server
<ADDRESS>	The IP address of the switch

For example, you can enter the command

```
upload config 45.1.12.101 extreme/<NAME>.cfg
```

and the macro substitutes the name of each switch on which it executes the macro.

These variables can only be used in macros, not in an interactive Telnet session.

- 3 To set the macro so that it plays back repeatedly at a specified interval, click the **Repeating** check box, and enter an interval (in seconds) in the Repeat Delay field.
- 4 Click **Play** to initiate playback of the macro on the selected switches. This opens a connection to the switch, logs in using the switch login and password as specified in the Inventory Manager, and runs the macro.

If the macro is a repeating macro, it will run repeat sequentially on all selected switches until you click **Cancel**.

The Macro Status column in the Telnet Connections table indicates the status of the macro as execution progresses on the selected switches. The four states are:

- **Pending**—the macro is intended to run on this switch, but has not yet started.
- **Playing**—the macro is currently running.
- **Cancelled**—the macro was cancelled before it completed.
- **Complete**—the macro has completed running.

Note: *Macro play will be automatically stopped if you exit the ExtremeView applet (by selecting another applet or logging out) while a macro is running.*

The Telnet session is usually left open after the macros completes. However, ExtremeView only allows five Telnet sessions to be open concurrently. Therefore, if you select more than five switches for macro playback, ExtremeView will open five connections, the close the oldest (first connection) in order to open a connection on the sixth switch, and so on. When macro playback has completed on all the selected switches, the Telnet sessions will be left open on the last five.

5 To close an open connection, select the switch and click the **Closed** button.

To view the results of the macro execution on a particular switch, select the switch in the Telnet switch list in the Component Tree. This will display a telnet session display for the switch. Because it displays an active telnet session, you can use this page to view the progress of the macro as the various ExtremeWare commands are executed.

RUNNING AN INTERACTIVE TELNET SESSION ON AN INDIVIDUAL SWITCH

You can open a Telnet session on an individual switch, and execute commands interactively by selecting the switch from the Telnet switch list in the Component Tree. This opens a Telnet session to the selected switch, and then waits for command input, just as with any other Telnet session.

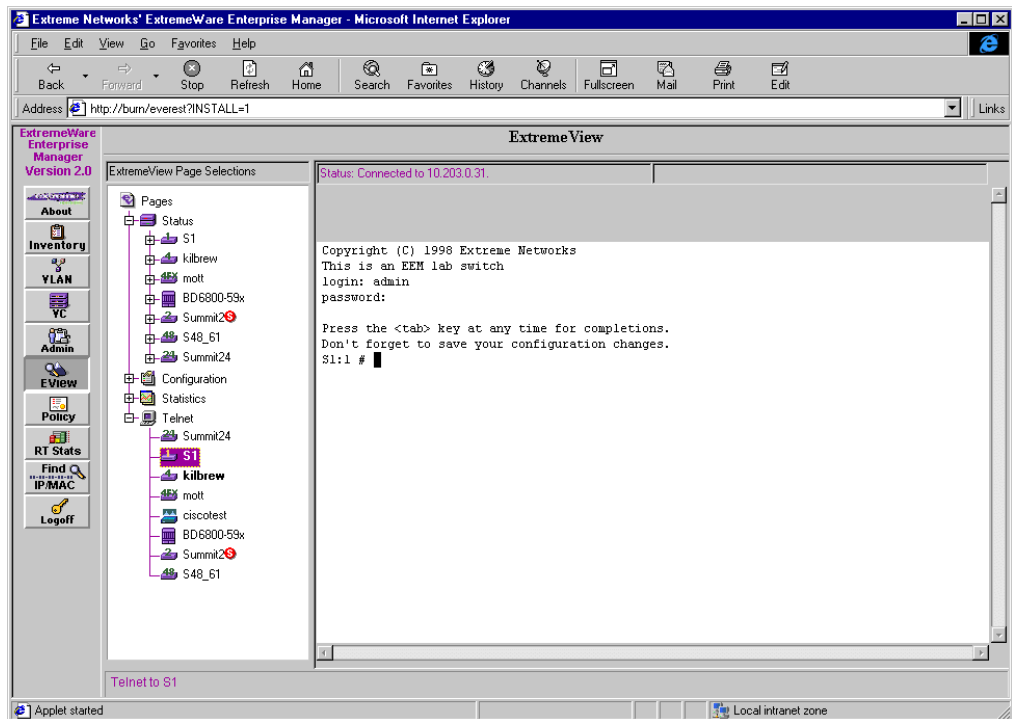


Figure 6-11: An open Telnet session for a switch in the ExtremeView applet

The Telnet session window is a two-tone window—the bottom of the window is white, the top is grey. The last 25 lines of Telnet commands and responses always appear in

the white portion of the window. As output grows, the older lines scroll up into the grey portion of the screen. This makes it easy to tell whether you are viewing the most recent Telnet output.

The Telnet session window will display the commands and results from macros that are run on the switch. You can also type in commands individually.

You cannot use the macro variables (<NAME>, <DATE>, <TIME>, <ADDRESS>) in a command you enter interactively.

COPY/PASTE FROM AN INTERACTIVE TELNET SESSION

A copy and paste function is available from an interactive Telnet session. Copy and paste lets you copy from one interactive Telnet session into another interactive session or into the Macro Record/Play Buffer. It is implemented with commands on a pop-up menu displayed by using the right mouse button (see Figure 6-12).

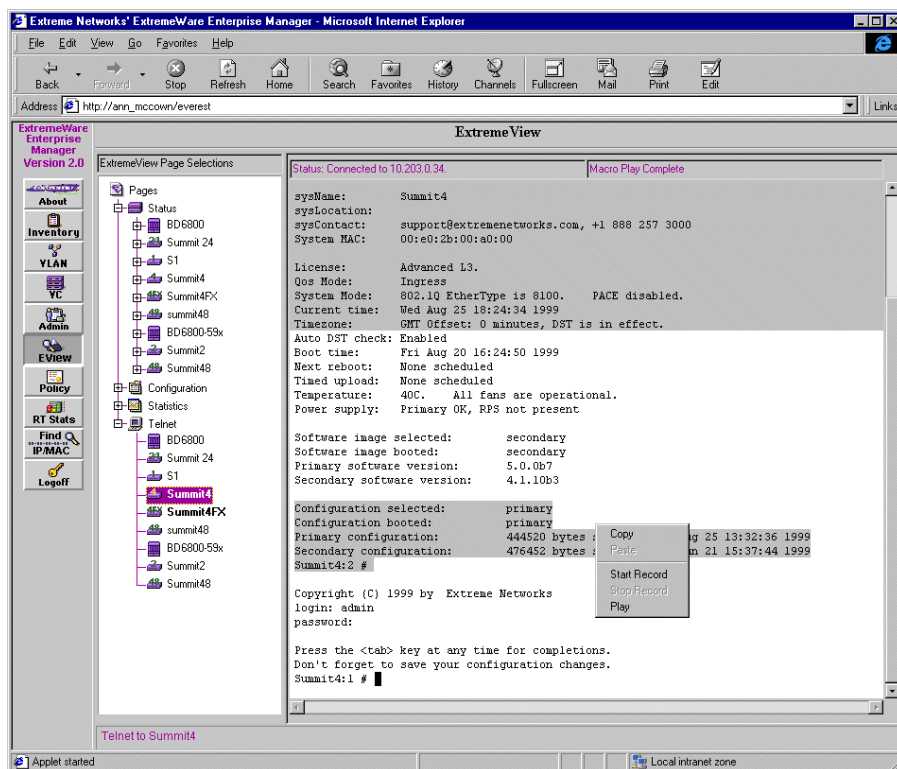


Figure 6-12: An open Telnet session for a switch in the ExtremeView applet

- To copy from an interactive session, highlight the lines you want to copy, click the right mouse button and select **Copy** from the pop-up menu.
- To paste into another window, display the window, place the cursor where you want the lines inserted, click the right mouse button and select **Paste** from the pop-up menu.

MACRO RECORDING AND PLAYBACK FROM AN INTERACTIVE TELNET SESSION

The Record function creates a macro by echoing commands you type in an interactive Telnet session, into the macro Record/Play Buffer. It is implemented with commands from a pop-up menu displayed by using the right mouse button (see Figure 6-12).

- To start recording a macro, click the right mouse button and select **Start Record** from the pop-up menu.
Everything you type after this until you select **Stop Record** from the pop-up menu, will be copied into the macro Record/Play Buffer.
- To stop recording a macro, click the right mouse button and select **Stop Record** from the pop-up menu.
- To play back the macro to multiple switches, select **Telnet** in the Component tree, and play back the macro in the main Telnet page as discussed in the section “Running ExtremeWare Command Macros” on page 6-11.
- To play the macro on an individual switch, select the switch in the Component Tree to display its interactive telnet session, click the right mouse button, and select **Play** from the pop-up menu.

USING TELNET WITH CISCO DEVICES

You can open an interactive Telnet session on a Cisco device and execute commands interactively. Select the switch from the Telnet switch list in the Component Tree. This opens a Telnet session to the selected switch, and waits for command input, just as with any other Telnet session (see Figure 6-12).

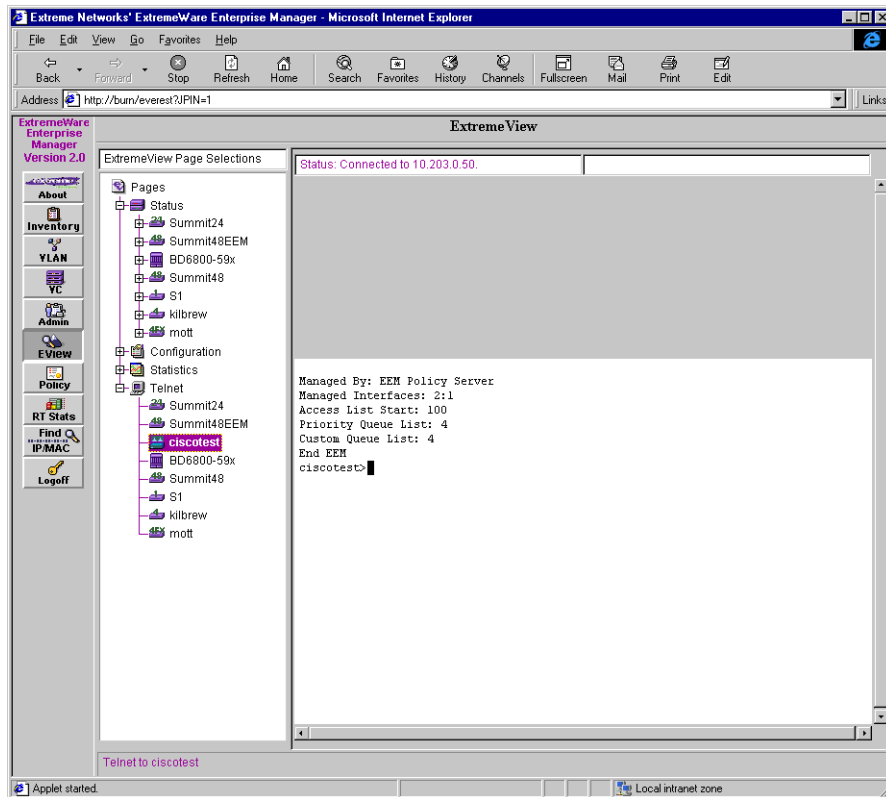


Figure 6-13: An open Telnet session for Cisco device in ExtremeView

You can enter and execute commands using Cisco's Command Line Interface. The commands and any resulting output will be displayed in the session window just as if you were running a Telnet session on any other client.

The Telnet session window is a two-tone window—the bottom of the window is white, the top is grey. The last 25 lines of Telnet commands and responses always appear in the white portion of the window. As output grows, the older lines scroll up into the grey portion of the screen. This makes it easy to tell whether you are viewing the most recent Telnet output.

The copy and paste feature, macros, and the macro variables (<NAME>, <DATE>, <TIME>, <ADDRESS>) are not supported for Cisco devices.

7

Using the VLAN Manager

This chapter describes how to use the VLAN Manager for:

- Viewing enterprise-wide, tagged and untagged VLAN information for Extreme (Summit and BlackDiamond) switches managed by the ExtremeWare Enterprise Manager
- Adding new tagged or untagged VLANs to Extreme devices, adding ports to those VLANs, and modifying IP addresses
- Deleting VLANs
- Modifying VLANs
- Adding and deleting protocol filters

OVERVIEW OF VIRTUAL LANs

A Virtual LAN is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN). Extreme switches have a VLAN feature that enables you to construct broadcast domains without being restricted by physical connections.

The VLAN Manager creates and manages VLAN for Extreme Networks devices only. It does not handle other third-party devices, even though some third-party devices (Cisco and Xedia devices as of ExtremeWare Enterprise Manager 2.0) can be managed through the Inventory Manager.

The VLAN Manager is an enterprise-wide application that manages all aspects of VLANs on Extreme devices. If you run the Enterprise Manager with Administrator or Manager access, you can:

- Create and delete VLANs
- Add or remove ports from existing VLANs
- Modify a VLAN's IP address
- Enable/disable IP Forwarding
- Create and modify the protocol filters used to filter VLAN traffic

Extreme switches support a maximum of 256 VLANs. VLANs on Extreme switches can be created according to the following criteria:

- Physical port
- 802.1Q tag
- Protocol sensitivity using Ethernet, LLC SAP, or LLC/SNAP Ethernet protocol filters
- A combination of these criteria

In the Enterprise Manager, a VLAN is defined uniquely by its

- Name
- 802.1Q tag (if defined)
- Protocol filters applied to the VLAN

As a result, multiple switches are shown as members of the same VLAN whenever all the above are the same.

For a more detailed explanation of VLANs, see the chapter “Virtual LANs (VLANs)” in the *Summit Switch Installation and User Guide*.

DISPLAYING VLANs

When you click the VLAN icon in the ExtremeWare Enterprise Manager Navigation Toolbar, the VLAN Manager window is displayed, as shown in Figure 7-1.

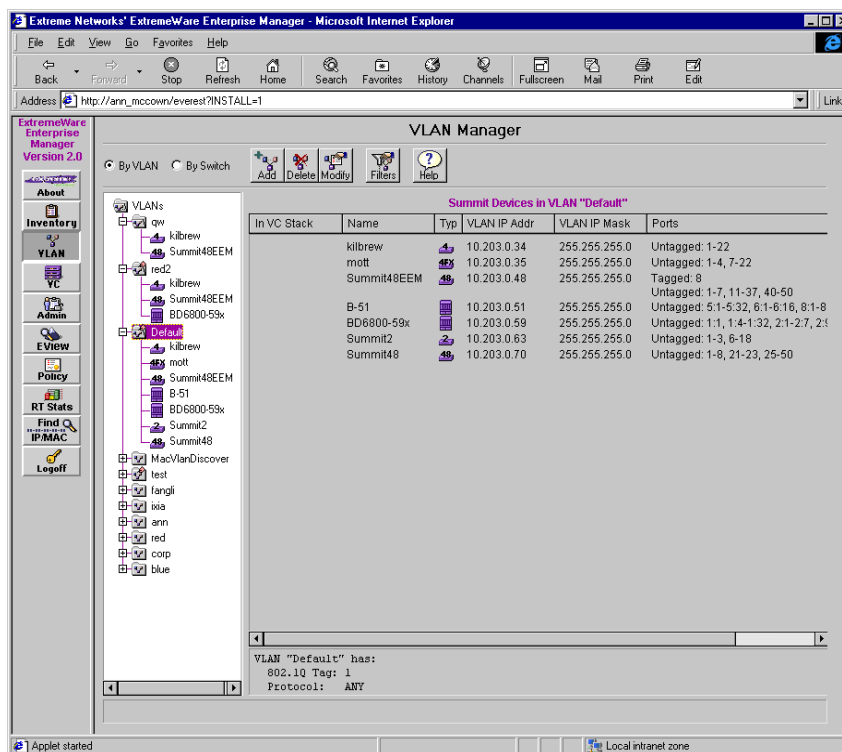


Figure 7-1: VLAN Manager applet, topology shown by VLAN

The VLANs currently known to the Enterprise Manager database are displayed in the Component Tree on the left. The panel on the right shows summary information about the configuration of the switches and ports that are members of a selected VLAN.

Note: *You must add switches to the ExtremeWare Enterprise Manager database through Discovery or by using the Add function in the Inventory Manager. Until you add a switch to the database, you cannot create any VLANs on that switch.*

Information about VLAN configurations is obtained when a switch is added to the database.

The VLAN Manager can display information either by VLAN (showing all the switches with ports that are members of a specific VLAN) or by switch (showing the VLANs that have members on a specific switch).

- Select **By VLAN** to display VLANs in the component tree, and showing under the VLAN each switch that has ports that are members of the VLAN (see Figure 7-1).
- Select **By Switch** to display every switch in the component tree, and showing under the switch each VLAN that “owns” ports on the switch, as shown in Figure 7-2.

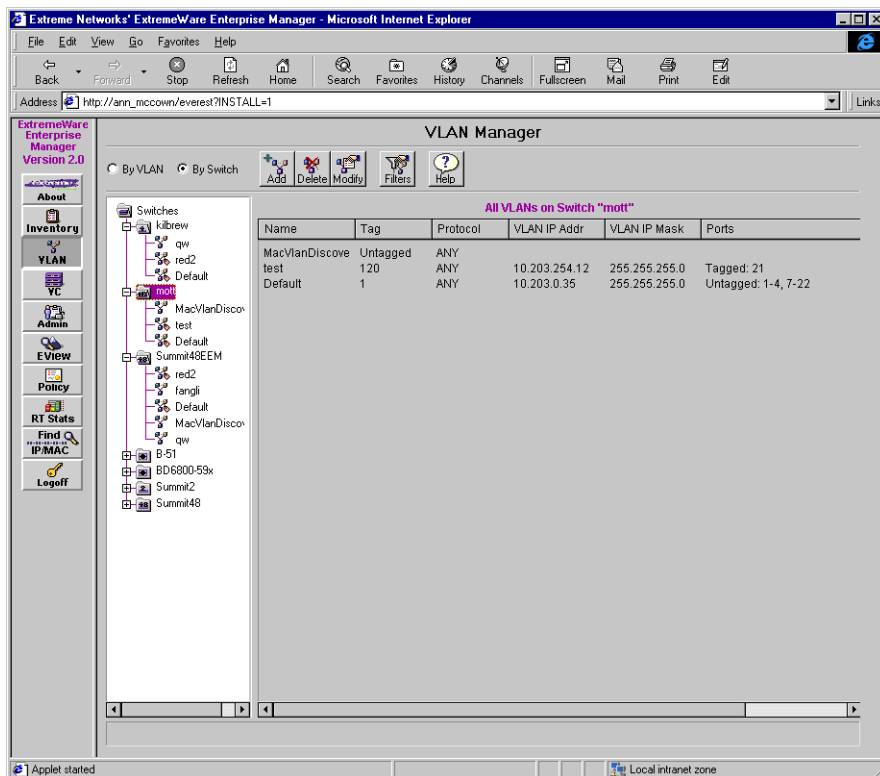


Figure 7-2: VLAN topology shown by switch

You can display details about the component ports of a VLAN by selecting the VLAN or switch in the tree on the left. The panel on the right displays detailed information about the selected component, as shown in Figure 7-3 and Figure 7-4.

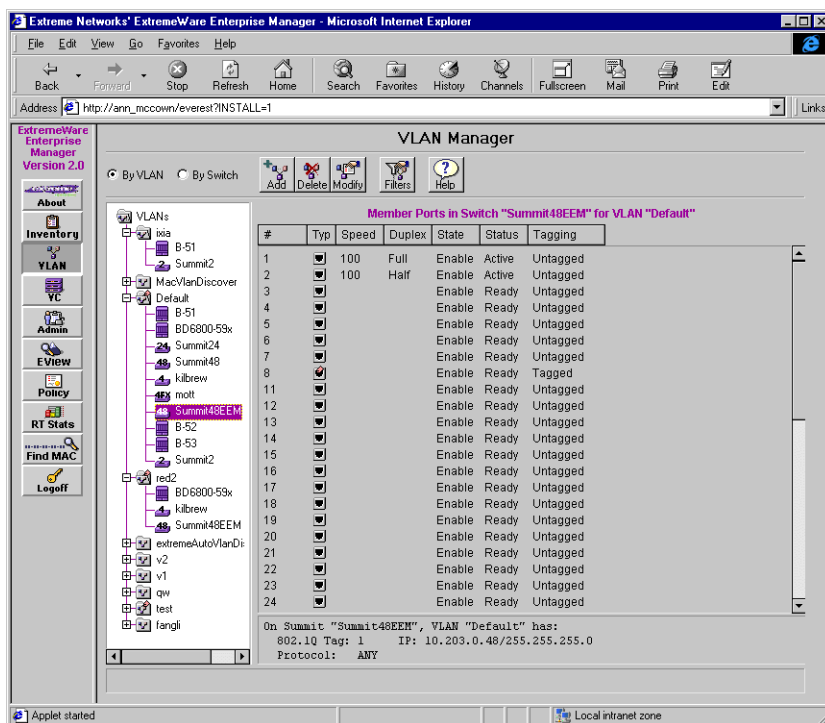


Figure 7-3: VLAN member ports on a selected switch

Figure 7-3 presents details about which ports in a VLAN belong to the selected switch.

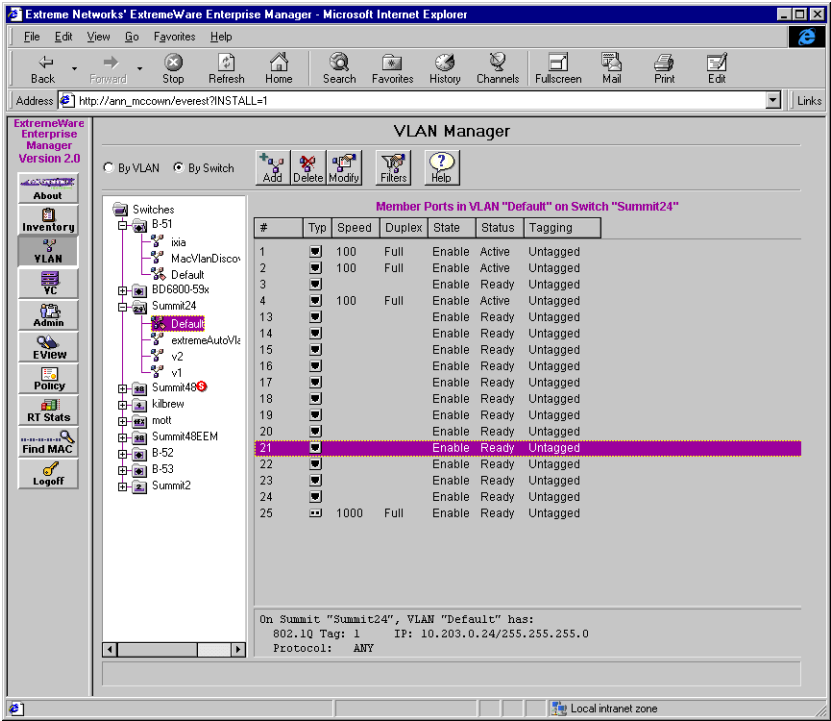


Figure 7-4: Switch member ports for a selected VLAN

Figure 7-4 presents details about which ports on a given switch are found in the selected VLAN.

ADDING A VLAN

Users with Administrator or Manager access can create VLANs on the Extreme switches managed by the ExtremeWare Enterprise Manager. If you have Monitor access only, you can not use this function.

To add a new VLAN, do the following:

- 1 Click the **Add** button in the VLAN Manager panel.

The Add VLAN dialog box, Properties & Ports page is displayed, as shown in Figure 7-5.

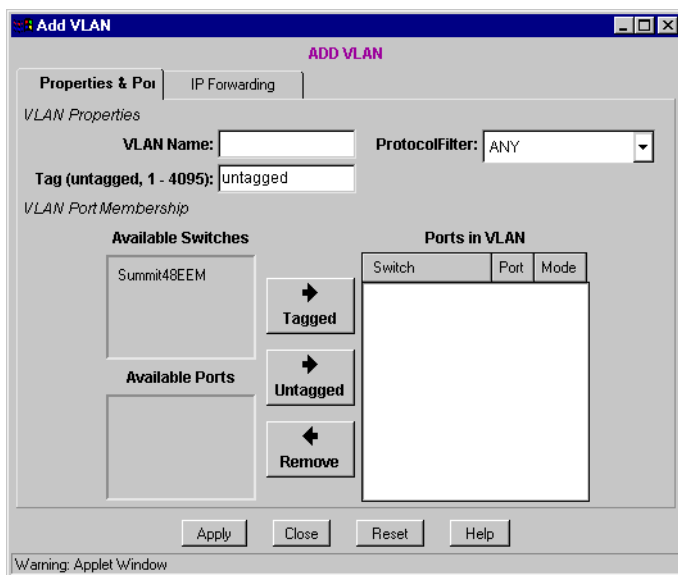


Figure 7-5: Add VLAN dialog, Properties and Ports page

- 2 Enter a descriptive name for the VLAN. The name must begin with a letter followed by up to 31 characters. See the *Summit Switch Installation and User Guide* for details on VLAN naming.
- 3 Select an entry from the pull-down **Protocol Filter** list. This selection determines what protocol (if any) is used to determine membership in this VLAN. If you do not want to specify a protocol, select **ANY**. This means the filtering rules will match all unfiltered protocols.
- 4 If the VLAN is to be tagged, enter a 802.1Q tag value in the **Tag** field. The tag value can be a number between 2 and 4095. By entering a tag number, you enable tagging for this VLAN. Enter the text “untagged” or 0 (zero) to indicate that the VLAN is to be untagged.
- 5 To add a port to the VLAN, first select the switch from the **Available Switches** list. This displays a list of ports on the switch that are available to be included in the VLAN.

Note: *The **Available Ports** list does not include ports in SummitLink™ mode, or ports configured as slave load sharing ports.*
- 6 Select a port from the **Available Ports** list.

- 7 Click **Tagged** to add the port as a tagged port. Click **Untagged** to add the port as an untagged port.

Note: *If this is an untagged VLAN, you are not able to add a tagged port.*

When you add an untagged port to a VLAN, it is automatically removed from any other VLAN which uses the same protocol as the new VLAN, and where the port is an untagged member.

You can add a switch to a VLAN as a unit—just select the switch without selecting any ports, and click **Tagged** or **Untagged** to add the switch to the VLAN.

- 8 To remove a port from the VLAN, select the port from the Ports in VLAN list, and then click **Remove**.
- 9 When you have finished adding ports to the VLAN, click **Apply** to have the changes take effect.

The VLAN is created on the switches whose ports are members of the new VLAN.

Once you have added a VLAN, you can specify an IP address and mask for the VLAN on each switch, and also enable or disable IP Forwarding.

- 1 To select the IP Forwarding tab at the top of the Add VLAN window.

The IP Forwarding page is displayed, as shown in Figure 7-6.

Add VLAN

ADD VLAN

Properties & Port | **IP Forwarding**

Please enter a VLAN in the "Properties & Port" tab first.

Switch	VLAN IP address	VLAN IP mask	IP forwarding	Gateway

Please select a row from the above table to configure.

IP address: IP mask:

☐ Enable IP forwarding

Apply Close Reset Help

Warning: Applet Window

Figure 7-6: Add VLAN dialog, IP Forwarding page

- 2 Select a switch from the table of switches.
- 3 Enter an IP address and IP mask. Click the Enable IP Forwarding check box if you want to enable IP forwarding for this VLAN on the switch.
- 4 Click **Apply** to have the changes take effect.

DELETING A VLAN

Users with Administrator or Manager access can delete VLANs from the Extreme switches managed by the ExtremeWare Enterprise Manager. If you have Monitor access, you will not be able to use this function.

To delete a VLAN, follow these steps:

- 1 Click the **Delete** button in the VLAN Manager panel.

The Delete VLAN dialog is displayed, as shown in Figure 7-7.

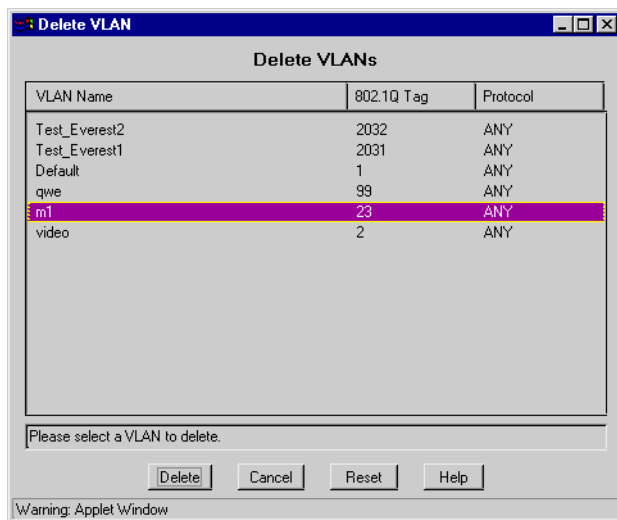


Figure 7-7: The Delete VLAN page

- 2 Select the VLAN you want to delete
- 3 Click **Delete**.

The VLAN is deleted from all the switches on which it exists.

MODIFYING A VLAN

Users with Administrator or Manager access can modify the properties of a VLAN, and add and remove ports from the VLAN. If you have Monitor access, you will not be able to use this function.

To modify a VLAN, follow these steps:

- 1 Click the **Modify** button in the VLAN Manager panel.

The Modify VLAN dialog, Properties & Ports page is displayed, as shown in Figure 7-8.

Modify VLAN

Properties & Ports | IP Forwarding

VLAN Properties

VLAN Name: red2 Protocol Filter: IP

Tag (untagged, 1 - 4095): 345

VLAN Port Membership

Available Switches

- kilbrew
- mott
- Summit48EEM
- B-51

Available Ports

Ports in VLAN

Switch	Port	Mode
kilbrew	4	tagged
mott	7	tagged
Summit48EEM	8	tagged
B-51	2:4	tagged

Buttons: Tagged, Untagged, Remove, Apply, Close, Reset, Help

Figure 7-8: The Modify VLAN dialog, Properties and Ports page

- 2 Select a VLAN from the drop-down list in the **VLAN Name** field.

The current values for the VLAN are displayed.

Note: The **Ports in VLAN** list does not display SummitLink ports, because you cannot modify them.

- 3 To change the Protocol Filter selection, select a different entry from the pull-down **Protocol Filter** list.
- 4 To change the VLAN tag, type a new value into the **Tag** field.
To disable tagging for the VLAN, type “untagged” or 0 (zero) into the **Tag** field.

- 5 To remove a port from the VLAN, select the port in the **Ports in VLAN** list, and click **Remove**.

- 6 To add a port to the VLAN, first select the switch from the **Available Switches** list. This displays a list of ports on the switch that are available to be included in the VLAN.

Note: *The **Available Ports** list does not include ports in SummitLink mode, or ports configured as slave load sharing ports.*

- 7 Select a port from the **Available Ports** list.
- 8 Click **Tagged** to add the port as a tagged port. Click **Untagged** to add the port as an untagged port.

Note: *If this is an untagged VLAN, you will not be able to add a port as a tagged port.*

If a port is added as an untagged port, it is automatically removed from any other VLAN which uses the same protocol as the new VLAN, and where the port is an untagged member.

You can add a switch to a VLAN as a unit—just select the switch without selecting any ports, and click **Tagged** or **Untagged** to add the switch to the VLAN.

- 9 When you have finished adding and removing ports, click **Apply** to have the changes take effect.

If all ports of a switch are removed from the VLAN, the VLAN is deleted from that switch.

If a port on a new switch is added to the VLAN, then the VLAN is created on that switch.

- 10 To modify the IP address and mask for a VLAN on a switch, and to enable or disable IP Forwarding, select the IP Forwarding tab at the top of the Add VLAN window.

The IP Forwarding page is displayed, as shown in Figure 7-6.

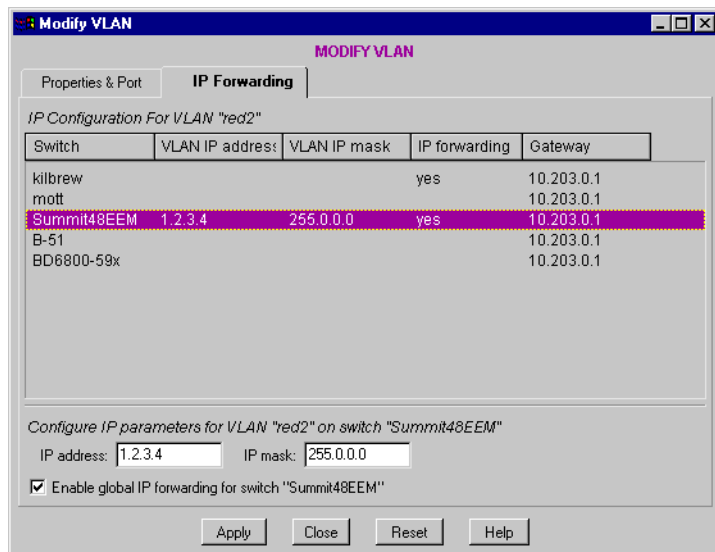


Figure 7-9: The Modify VLAN dialog, IP Forwarding page

- 11** Select a switch from the table of switches.
- 12** Change the IP address and IP mask as appropriate. Click the Enable IP forwarding check box to enable or disable IP forwarding for this VLAN on the switch.
- 13** Click **Apply** to have the changes take effect.

ADDING AND DELETING PROTOCOL FILTERS

Users with Administrator or Manager access can view, add, and delete protocol filter definitions. If you have Monitor access, you can view filter definitions, but not add or delete them.

To view, delete or add protocol filter definitions, do the following:

- 1** Click **Protocol Filters** in the VLAN Manager.

The View/Delete page of the Protocol Panel dialog box is displayed, as shown in Figure 7-10.

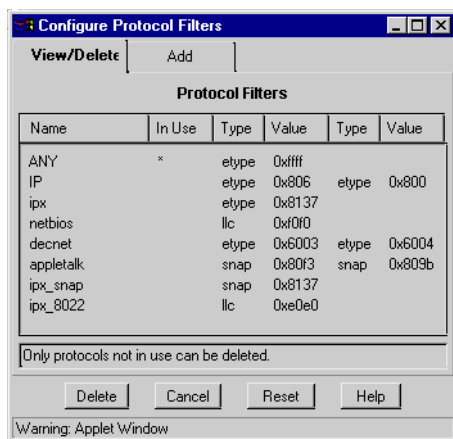


Figure 7-10: Protocol Panel dialog box, View/Delete page

This page shows all the protocol filters configured within the ExtremeWare Enterprise Manager. Any filters that are in use by a VLAN are indicated with an asterisk (*) in the In Use column.

- 2 To delete a protocol filter, select a filter in the list, and click **Delete**.

This deletes the protocol filter from all Extreme switches managed by the ExtremeWare Enterprise Manager, as well as from the Enterprise Manager database.

Note: *If a filter is in use by a VLAN, you will not be able to delete it.*

To add a protocol filter, follow these steps:

- 1 Click the **Add** tab at the top of the Protocol Panel dialog box to display the Add Protocol page, as shown in Figure 7-11.

Figure 7-11: Protocol Panel dialog box, Add Protocol page

- 2 Enter a descriptive name for the Protocol. The name must begin with a letter followed by up to 31 characters. See the *Summit Switch Installation and User Guide* for details on naming.
- 3 Select a protocol type from the pull-down list in the **type** column.
- 4 Type a corresponding four-digit hexadecimal filter value in the **value** field.
- 5 Repeat steps 3 and 4 to enter up to six type-value pairs.
- 6 When you have finished entering the definition, click **Add** to add the new protocol filter to the Enterprise Manager database.

Note: *The protocol filter is now available to be used on any switch, but is not created on any switches at this time. The protocol filter is created on a switch only when you create or modify a VLAN to use the new protocol filter on that switch. The database acts as a collective store for network data without needing to replicate it on every switch.*

8

Using the Policy System

This chapter describes how to use the ExtremeWare Enterprise Manager Policy System for:

- Creating, modifying, and deleting network Quality of Service (QoS) policies
- Defining and modifying QoS treatments
- Defining users and user groups as policy objects
- Defining end stations and end station groups as policy objects
- Configuring network devices with the defined network policies
- Importing users, user groups, and end stations from Windows NT Domain Controller or Solaris NIS

OVERVIEW OF THE POLICY SYSTEM

Policy-based management is used to protect and guarantee delivery of mission-critical traffic.

A network policy is a set of high-level rules for controlling the priority of, and amount of bandwidth available to, various types of network traffic. Through ExtremeWare Enterprise Manager, policies can be defined in terms of individual users and desktop systems, not just by IP or MAC addresses, ports, or VLANs.

The ExtremeWare Enterprise Manager Policy System lets you work with high-level policy objects (users, desktop systems, groups of users or systems, applications, and groups of devices and ports) in defining policies. The policy system translates those policy objects into the specific information needed for QoS configuration of network

devices. It also detects overlaps and conflicts in policies, with precedence rules for resolving conflicting QoS rules.

Note: *The ExtremeWare Enterprise Manager Policy System is based on the ExtremeWare 5.0's Policy-Based QoS. For details on the capabilities and implementation of QoS in Extreme Switches, see the chapter on Quality of Service in the ExtremeWare Software User Guide V 4.0, and the Release Note for ExtremeWare 5.0.*

POLICY TYPES

The ExtremeWare Enterprise Manager Policy System supports several types of policies:

- **Application Server Policy** maps a QoS treatment to traffic moving to and from an application on a particular server connected to a port on an Extreme switch. You only need to specify the application (which translates to a well-known Layer 4 port) and server when you create the policy, and the Policy System maps this to the appropriate port. As shown in Figure 8-1 below, the policy you specify is implemented as Source Port QoS on the traffic outbound from source port, and as IP QoS for the traffic inbound to via source port to the server.

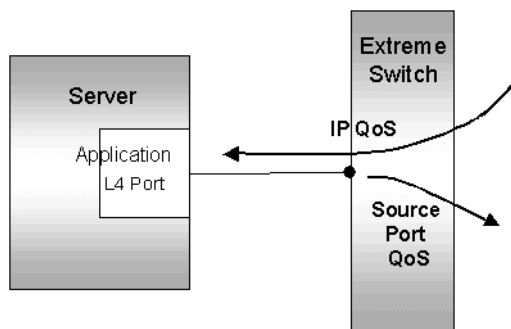


Figure 8-1: Application Server Policy

For an application server policy, you can specify only one application (e.g. HTTP, FTP, Baan) as the endpoint, but multiple servers (not shown in the illustration) if they are all running the specified application. The exception is if you select “ANY” as the application, in which case the Policy System will use the IP address alone as the endpoint (without a Layer 4 port) for every server you specify. This is discussed in more detail in the section “Application Server Policy Definition Tab” on page 8-24.

- **Client/Server Policy** maps a QoS treatment to traffic going between a server and specific clients. You specify the both sets of endpoints (clients and server) between which the traffic will travel. The server endpoint can include an application (translated to an L4 port) or it can be a host (indicated by the application choice “ANY,” translated to an IP address only). The Policy System determines the switches that should be affected by this policy. As shown in Figure 8-2 below, the policy you specify is implemented as IP QoS in both directions between the client and server. Although not shown in the diagram, you can specify multiple servers as well as multiple clients.

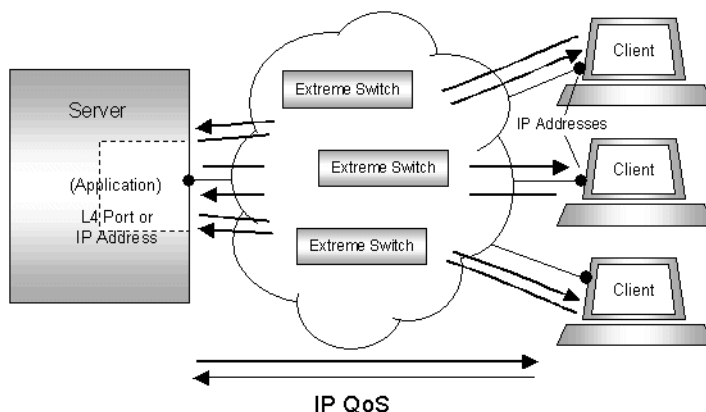


Figure 8-2: Client/Server Policy

For a client/server policy, as with an application policy, you can specify only one application (e.g. HTTP, FTP, Baan) as the endpoint, but multiple servers (not shown in the diagram). In addition, you can select multiple client endpoints, and the Policy System will generate IP QoS rules that it will apply to traffic bi-directionally along the entire route between server and client.

Note that the potential combination of traffic flows can get very large if you specify a large number of clients and servers in a client/server policy. This is discussed in more detail in the section “Client/Server Policy Definition Tab” on page 8-27.

- **Source Port Policy** maps a QoS treatment to traffic from a specific port on an Extreme switch. You specify the specific ingress ports from which the traffic will originate. As shown in Figure 8-3 below, a source port policy is uni-directional, and implements Source Port QoS on the flow from the specified source port.

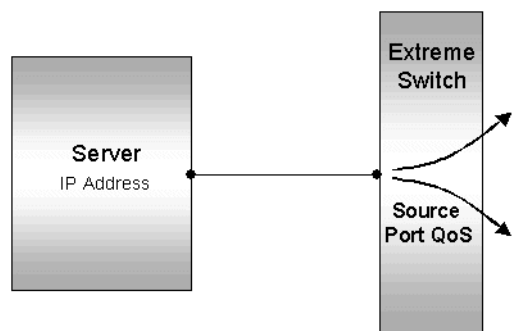


Figure 8-3: Source Port Policy

You can specify multiple source ports in a single policy, and you can specify them by providing a host name or even a user name (or group of names) and leave it to the Policy System to determine the source port to which those names map. For more details, see the section “Source Port Policy Definition Tab” on page 8-30.

- **VLAN Policy** maps a QoS treatment to traffic from one or more VLANs. You specify the VLANs from which the traffic will originate, and the Policy System maps this to the switches and ports involved. As shown in Figure 8-4 below, the Policy System implements VLAN QoS for all the traffic flows from the specified VLANs. In the illustration, a VLAN Policy has been specified for VLAN A, but not for VLAN B.

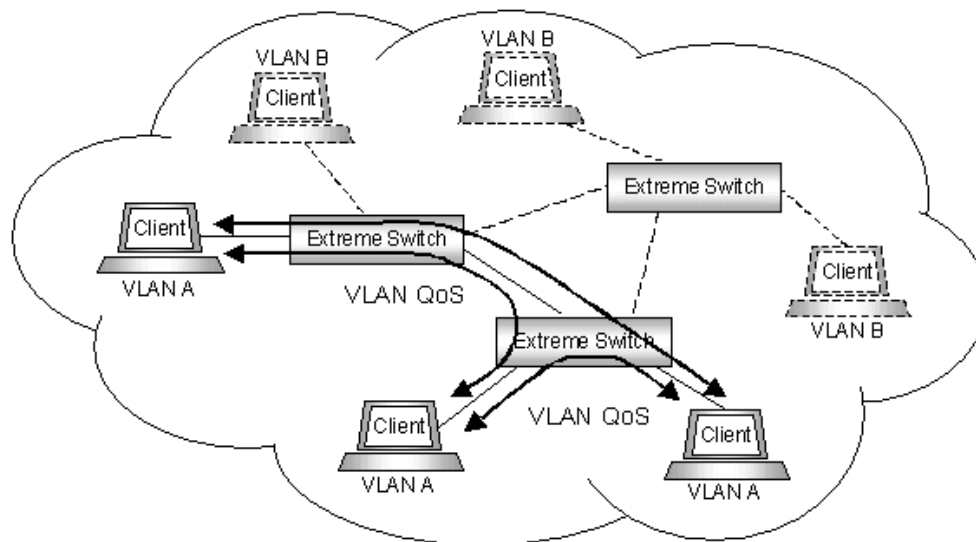


Figure 8-4: VLAN Policy

Both VLAN QoS and Source Port QoS depend on 802.1Q tagging to carry the QoS parameters across VLAN boundaries or switch boundaries. In order to allow these QoS types to be effective end-to-end, you should make sure your switch-to-switch links use tagged ports.

- **Custom Policy** lets you specify the components for an IP-based policy, without any predefinition of relevant policy components.

Each policy type (except for Custom) acts as a template by predefining certain components of the policy. For example, in an Application policy, only endpoints for one side of the policy need to be entered. The other side of the policy is always “ANY” and the traffic direction is always bi-directional.

BASIC POLICY DEFINITION

A QoS policy in the ExtremeWare Enterprise Manager Policy System is defined as shown in Figure 8-5.

A policy is composed of:

- A name and description that you supply when you create the policy.
- Definitions of the origin and destination of the traffic affected by the policy. This can be defined as endpoints using the set of policy objects described below (see “Policy Objects”), or as an application or L4 port.
- The traffic direction (which is predefined for some of the policy types).
- The treatment to be applied.
- The implementation type (IP QoS, Source Port QoS, or VLAN QoS), which also may be predefined based on the policy type or endpoint types.

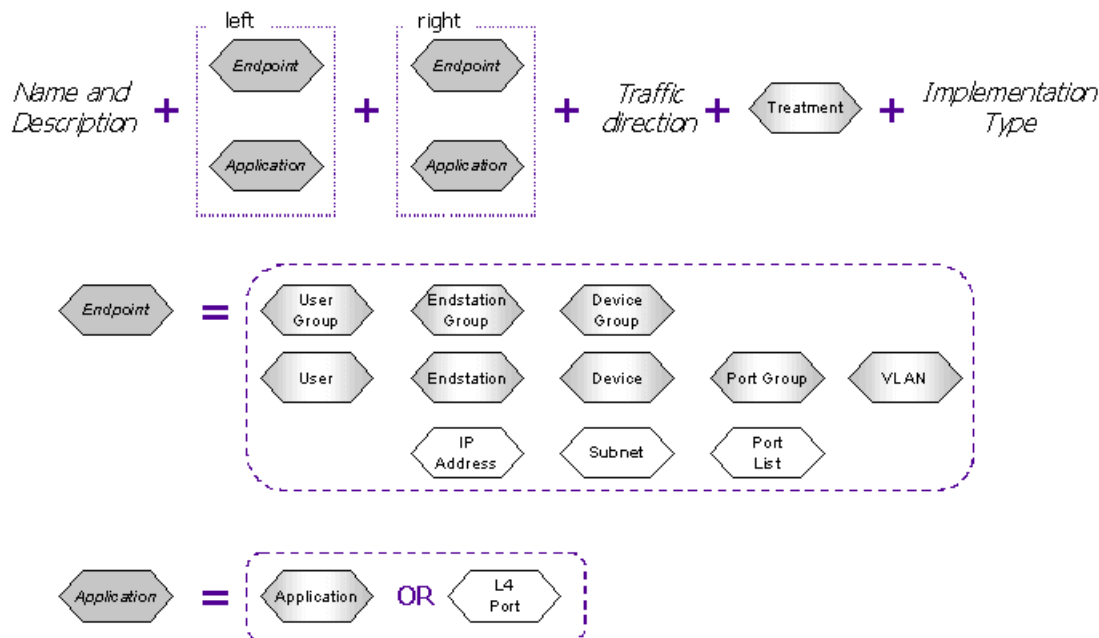


Figure 8-5: Basic Policy Definition

The ExtremeWare Enterprise Manager Policy System converts the high-level policy definition you supply into a set of low-level QoS rules that it will implement on the devices within the policy's scope. To do this, the Policy system takes the following steps:

- 1 Converts the endpoint components, application components, and traffic direction components into traffic patterns.
- 2 Converts the policy treatment into QoS profiles.
- 3 Combines the traffic patterns and QoS profiles into QoS rules.
- 4 Uses the policy scope to determine to which device(s) the QoS rules should be applied (see "Policy Scoping").
- 5 Resolves any QoS rule conflicts using precedence relationships.
- 6 Configures the QoS rules on the network switches either automatically (if Auto Configuration is on) or when you initiate the configuration using the Configuration page.

POLICY OBJECTS

The ExtremeWare Enterprise Manager Policy System lets you work with high-level components, or policy objects, when defining a QoS policy. The components used within the Enterprise Manager Policy System are the following:

- **Devices** (by name) and **Device Groups**: These are entered into the Enterprise Manager database via the Inventory Manager (Discovery or Add Devices), and are mapped to IP addresses in the Enterprise Manager database.
- **End Stations** (by name) and **End Station Groups**: These are entered into the Policy System, through the Import capability or individually using the GUI. End Station Groups are sets of individual End Stations that are grouped to allow them to be acted upon as a unit. The individual End Stations are mapped to IP addresses through Network Name Lookup Services, or can be mapped manually using the GUI. Within the Policy System the IP addresses are mapped to physical ports on an Extreme switch using DLCS, or the mapping can be specified manually.
- **Users** (by name) and **User Groups**: These are also entered into the Policy System, through the Import capability or individually using the GUI. User Groups are sets of individual Users that are grouped to allow them to be acted upon as a unit. The individual Users are mapped to End Stations, either via DLCS or manually using the GUI. The End Stations are then mapped to IP addresses and physical ports as described above.
- **Port Groups**: These are defined in the Inventory Manager, and enable a set of ports (from different devices, if appropriate) to be acted upon as a group.
- **VLANs**: These are detected by the Enterprise Manager, and can also be created and modified using the VLAN Manager applet. They cannot be modified within the Policy System.
- **Subnets**: Subnet specifications can be used within a Custom Policy definition. They must be entered manually using the dotted quad notation.
- **Applications**: These are named entities (such as Baan, FTP, HTTP) that map to Layer 4 well-known ports. They cannot be modified within Enterprise Manager.
- **Treatments**: These are definitions of priority, minimum and maximum bandwidth that are combined with an application or a set of end point components to define a policy. Treatments are predefined, but they can be modified within the Policy System GUI.

These policy objects must be defined before they can be used in a policy. IP addresses, Layer 4 ports, and subnets can be typed directly into a policy without any pre-definition.

POLICY IMPLEMENTATION TYPES

ExtremeWare 5.0, and thus ExtremeWare Enterprise Manager, supports three policy implementation types. The implementation type of a policy is primarily determined by the type of endpoints to which the policy will apply.

The implementation types are:

- **IP QoS:** This uses IP addresses, or IP addresses plus Layer 4 ports, to define the sources and destinations of the traffic. All Client/Server policies, one direction of an Application Server policy, and Custom policies are implemented using IP QoS.
- **Source Port QoS:** This uses switch ports to define the sources of the traffic. Source Port policies, and the other direction of an Application Server policy, are implemented using Source Port QoS.
- **VLAN QoS:** This uses VLANs to define the sources and destinations of the traffic. A VLAN policy is implemented using the VLAN QoS mechanism.

You do not specify the implementation type—it is defined by the type and components of the policy you define.

Note: *Source Port QoS depends on 802.1Q tagging to carry the QoS parameters across switch boundaries, and VLAN QoS depends on tagging to carry QoS parameters across VLAN boundaries. To allow these QoS types to be effective end-to-end, you should make sure your switch-to-switch links use tagged ports.*

POLICY SCOPING

A policy may apply to the entire network (default behavior), or may be scoped to apply only to a portion of the network, by including and excluding device groups. In addition, treatments can have different parameters for different device groups. You specify the scoping when you create or modify a policy.

POLICY AUTO CONFIGURATION

The ExtremeWare Enterprise Manager Policy System supports auto-configuration of QoS policies. If Automatic Configuration is turned on every change you make within the ExtremeWare Enterprise Manager will trigger an immediate re-computation and reconfiguration of the QoS policies on your network. Configuration changes on a device managed by ExtremeWare Enterprise Manager, or a user login or end station reboot when DLCS is enabled, also trigger a recomputation and reconfiguration of QoS policies.

If Auto Configuration is turned off you must explicitly perform the configuration process using the Configuration function in the Policy System Client.

THIRD-PARTY DEVICE SUPPORT

In addition to supporting Extreme Networks switches, ExtremeWare Enterprise Manager provides support for some third-party devices. As of ExtremeWare Enterprise Manager 2.0, these include:

- Cisco devices running IOS 11.2 or later
- Xedia devices running the Xedia 2.1 R3 or later software

Enterprise Manager supports policies on these devices that simulate the QoS policies supported for Extreme devices. Policies on third-party devices are implemented as IP QoS policy rules.

CISCO DEVICE SUPPORT

ExtremeWare Enterprise Manager supports Cisco devices running Cisco IOS version 11.2. Later software versions may work but have not been tested. ExtremeWare Enterprise Manager 2.0 has been tested with the following models running Cisco IOS 11.2:

- Cisco 2500
- Cisco 3600
- Cisco 4000
- Cisco 7505

Other models may also work, but have not been tested. See the ExtremeWare Enterprise Manager Release Notes that accompanied your software for the most current list of supported models.

ExtremeWare Enterprise Manager uses a custom queue list for bandwidth control and a priority queue list for priority control. The custom or priority queue list are bound to each interface independently, so you can specify the queueing strategy individually for any given interface. You also specify the set of access lists, the custom queue list and the priority queue list for the ExtremeWare Enterprise Manager to use.

CISCO PORT MAPPINGS

When ExtremeWare Enterprise Manager pushes a policy to a Cisco device, the device automatically maps well-known TCP and UDP port numbers to names (for example, TCP port 80 to the name “HTTP”). When Enterprise Manager reads the rules from a Cisco device, it must re-map the name back to a port number. ExtremeWare Enterprise Manager uses a properties file to associate the well-known port names and port numbers. The file, `ciscoipports.properties`, is found in the `extreme` directory under the top-level installation directory

(`<eem-install-dir>/extreme/ciscoipports.properties`). If you encounter port-to-name mappings that are not included in this file, you can edit the file with a standard text editor. See Appendix E, “ExtremeWare Enterprise Manager Properties Files,” for a listing of this file as it shipped with ExtremeWare Enterprise Manager release 2.0.

LIMITATIONS ON CISCO DEVICE SUPPORT

There are certain policies that cannot be fully implemented on Cisco devices to make them function exactly like Extreme devices.

Maximum bandwidth parameter in a QoS profile. The maximum bandwidth parameter is not used when ExtremeWare Enterprise Manager pushes policies to Cisco devices.

QoS rule precedence. When two policies specify overlapping traffic streams that are each associated with different profiles, and neither stream is a proper subset of the other, (for example, one is source IP: 10.203.1.1, destination IP: 10.203.1.2 and the other is HTTP traffic) then the resolution of which policy gets higher precedence is as follows:

Precedence	Profile
Highest	Blackhole
•	QP4
•	QP3
•	QP2
Lowest	QP1

For Extreme switches, there is a set of rules to determine the precedence. See the *ExtremeWare Software User Guide, V 4.0*, Chapter 8, “Quality of Service (QoS)” for details.

XEDIA DEVICE SUPPORT

ExtremeWare Enterprise Manager can support certain Xedia devices running Xedia software version 2.1. Later software versions may work but have not been tested. ExtremeWare Enterprise Manager 2.0 has been tested with the following model running the Xedia 2.1 software:

- Xedia Access Point

See the ExtremeWare Enterprise Manager Release Notes that accompanied your software for the most current list of supported models.

ExtremeWare Enterprise Manager uses class-based queueing (CBQ) to implement policies on Xedia devices. When you initially attempt to add a Xedia device into the Enterprise Manager database, the Inventory Manager checks for the software version. If the software version is below 2.1, it is flagged as an error, and the device is not added to the Enterprise Manager inventory.

You must make sure that the root CBQ class exists on the output of the interface where policies are to be configured, and that the row-status is active. Enterprise Manager only creates CBQ classes that implement policies below the active root CBQ classes on the outputs of each interface. The root class must be named “root-output-tree”. By default, all the root classes with the name “root-output-tree” are created for each interface by the Xedia 2.1 software.

LIMITATIONS ON XEDIA DEVICE SUPPORT

There are certain policies that cannot be fully implemented on Xedia devices to make them function exactly like Extreme devices.

Zero minimum bandwidth parameter in QoS profile. When the minimum bandwidth parameter is set to zero, the priority parameter does not have any effect. Please refer to your Xedia product documentation for more details.

QoS rule precedence. When two policies specify overlapping traffic, and these two traffic streams are associated with different profiles, then the resolution of which policy gets higher precedence is as follows:

Precedence	Profile
Highest	Blackhole
•	QP4

Precedence	Profile
•	QP3
•	QP2
Lowest	QP1

For Extreme switches, there is a set of rules to determine the precedence. See the *ExtremeWare Software User Guide, V 4.0*, Chapter 8, “Quality of Service (QoS)” for details.

Root class bandwidth-allocation parameter. Under the Xedia 2.1 R3 software, for an ethernet interface, the root CBQ class is created by default with a value that is the same as the interface speed—the nominal bandwidth of the interface. For example if the ethernet interface is specified as 10 Mbps, then the root CBQ class is created with 10 Mbps as the bandwidth-allocation parameter. However, under congestion, the CBQ classes (for ethernet interfaces only) will not function if they are configured with a bandwidth allocation parameter that is *greater* than the *actual* bandwidth of the interface. You must change the bandwidth-allocation parameter for the root CBQ class to be *less* than the actual bandwidth of the interface.

For example, for a 10Mbps ethernet interface transporting small (64 byte) packets, the actual throughput may be only 7.2 Mbps. In this case you should set the bandwidth allocation parameter to a value that is approximately 3% below this actual bandwidth (6.8 Mbps) in order for the CBQ class configuration to be effective. For larger packets, the actual bandwidth will more closely approach the nominal bandwidth of the interface.

This limitation exists only for ethernet interfaces, in the Xedia 2.1 R3 software. Contact Xedia for additional information.

Managed Interface. CBQ classes are defined per interface. ExtremeWare Enterprise Manager tries to set up the same CBQ class hierarchy on every interface that has the root class “root-output-tree” and where the root class is active. If you do not want Enterprise Manager to manage a specific interface, you can remove the root class or make the root class inactive.

Ownership of the CBQ class hierarchy. For interfaces that you want ExtremeWare Enterprise Manager to manage, you should not create CBQ classes under the root class. If you do, the policies that Enterprise Manager puts on the Xedia device may not function.

USING THE POLICY SYSTEM

To invoke the Policy System, click the **Policy** button in the Navigation Toolbar. The Policy System main window is displayed (see Figure 8-6).

The Component Tree on the left shows the elements of the Policy System. The main applet frame shows the definition and function of each of these elements.

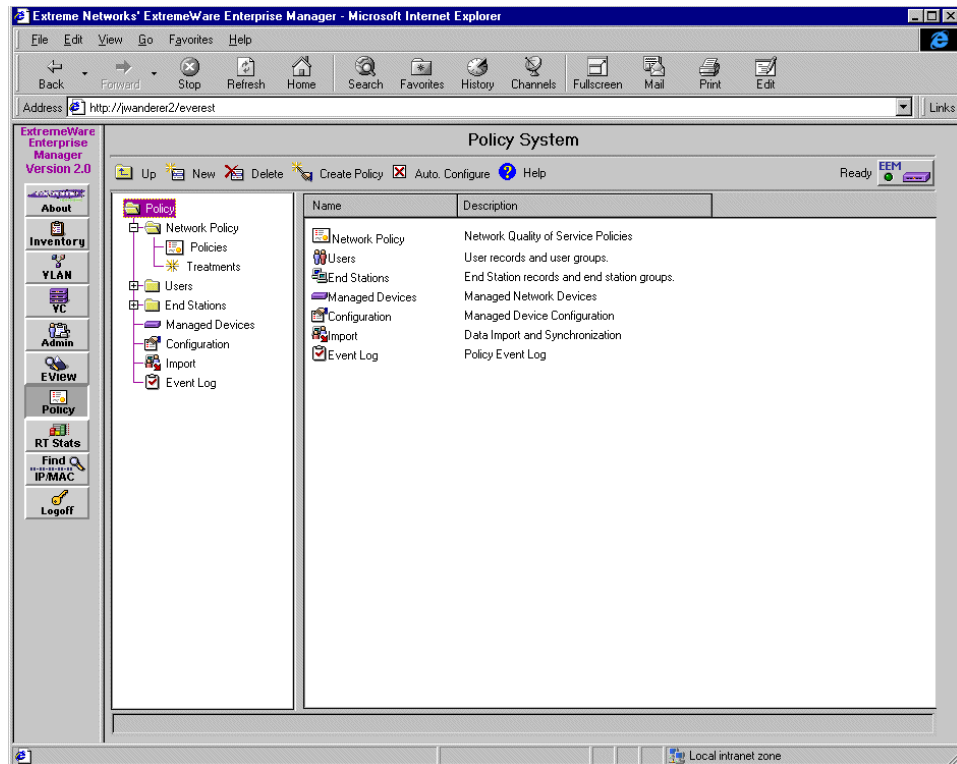


Figure 8-6: The Policy System main view

- **Network Policy** lets you display and define high-level policies that translate into the specific QoS rules operating within your enterprise network. You can define the overall policies and the treatments that can be used in a policy.
- **Users** lets you define individual users or groups of users as named policy objects for use in policy definitions. They dynamically translate into IP addresses/ports when QoS rules are computed for configuration onto network devices.

- **End Stations** lets you define specific hosts or groups of hosts by name as policy objects for use in policy definitions. They dynamically translate into IP addresses/ports when QoS rules are computed for configuration onto network devices.
- **Managed Devices** shows you all devices currently being managed by ExtremeWare Enterprise Manager. You can also set policy for Cisco devices using this function.
- **Configuration** lets you explicitly invoke the configuration of network devices based on the policies you've defined. This process lets you inspect the inputs and results of the QoS rule computation and configuration process before and after each step is completed. Auto-configuration must be turned off to use this function.
- **Import** lets you import users, user groups, and end-station definitions from a Windows NT domain controller or from a Solaris NIS server.
- **Event Log** displays a log of policy configuration commands and events.

Four buttons, a check box, and a Policy System State icon are provided at the top of the Policy System page. These are, from left to right:

- **Up**—moves you one level higher in the component tree.
- **New**—displays a menu from which you can choose to create a new Policy or policy object (User, User Group, End Station, End Station Group, or Port Set).
- **Delete**—lets you delete an item you've selected, after asking for confirmation.
- **Create Policy**—invokes a Policy Wizard that leads you through a set of interactive steps to create a network policy.
- **Auto. Configure**—a check ☒ in this box indicates that auto-configuration is turned on. An X ☐ in the box indicates that auto-configuration is turned off.
— Turn auto-configuration on or off by clicking the check box.

When auto-configuration is on, any changes made through the ExtremeWare Enterprise Manager, directly on the switches, or by events such as users logging in or out, will trigger automatic re-computation of QoS rules and re-configuration of the affected network devices. When auto-configuration is off, computation and configuration must be done explicitly from the Configuration page. This is discussed in more detail in the section “Configuring QoS Policies” on page 8-55.

- **Ready/Busy**—indicates the state of the Policy System. The state is Busy when the Policy System is computing QoS rules or configuring devices. Otherwise it is Ready.

CREATING A NEW NETWORK POLICY

There are two ways to create a network policy:

- Using the **Create Policy Wizard**, which is invoked by clicking the **Create Policy** button at the top of the Policy System page. The Create Policy Wizard guides you step by step through the policy creation process. This is recommended if you are new to using the Policy System.
- Selecting **Policy** from the **New** menu. This displays the **Create Network QoS Policy** view for the type of policy you want to create. The Network QoS Policy View lets you enter all the components of your chosen policy in a single form. This process is discussed in the section “Creating a Policy from the New Menu” on page 8-20.

USING THE CREATE POLICY WIZARD

To create a QoS policy using the **Create Policy Wizard**, follow these steps:

- 1 Click the **Create Policy** button at the top of the Policy System page.

The first page (**Name and Description**) of the Create Policy Wizard appears.

Follow the instructions on each page of the wizard as described below.

You can use the **Back** button to back up to a previous page and change your entries. You can go back to a previous page at any time until you click the **Finish** button, which is not available until you reach the last page of the wizard.

- 2 On the first page, enter a name for the policy (required) and a description of the policy (optional), then click **Next** to proceed to the next page.
- 3 On the **Policy Type** page, select the type of policy you want to create. The type of policy you choose will determine the type of information you will need to provide.

The policy type acts as a sort of template, requiring definition only of the components relevant to the particular policy type. You only need to define the variable policy components; components that are predefined for the policy type are included automatically. For example, for an Application Server policy, you only need to define the endpoints for one side of the policy; the other side is always “ANY” and the policy is always bi-directional.

- Application Server Policy lets you specify the components of a policy for traffic to and from a particular application and server.
- Client/Server Policy lets you specify the components of a policy for traffic between a server and specific clients.

- Source Port Policy lets you specify the components of a policy for traffic originating from specific ingress ports.
- VLAN Policy lets you specify the components of a policy for traffic originating from one or more VLANs.
- Custom Policy lets you specify the components for any other type of policy, without any predetermination of relevant policy components.

Note: In these steps, Client/Server has been selected as the policy type. The process is similar for other policy types.

- 4 Click **Next** to go to the **Client (s) - Server (s)** page, and specify the servers and clients that will determine the traffic flows to which this policy will apply.
 - a To select a server, click the policy object selector button (see Figure 8-7) at the right of the **Servers** field. You can specify the servers by using any of the available high-level objects: Users, User groups, End Stations, End Station Groups, or Devices. The Policy system will take policy objects you designate, along with an application (L4 port) if you designate one, and translate these into a set of IP addresses that will specify the server-side endstations for this policy.

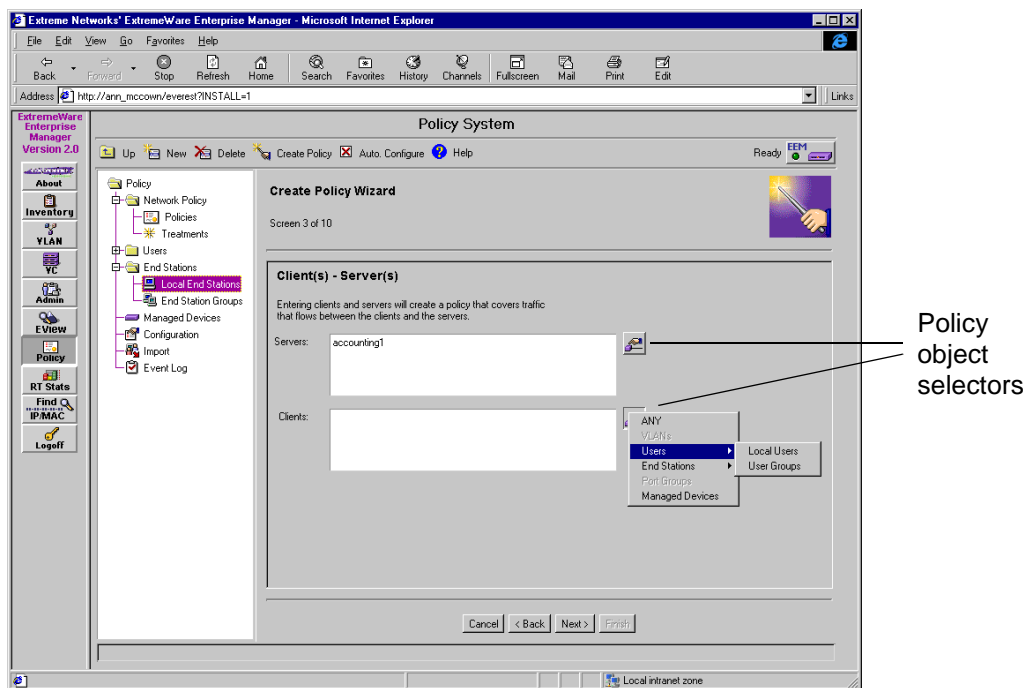


Figure 8-7: Using the policy object selector to specify policy components

- b Select individual users, user groups, end stations, end station groups, or devices and add or remove them from the Selected items list. You can display either the Local End Stations list or the End Station Groups list by selecting from the pull-down list in the **Show Type** field.

When you have finished, click **OK**.

You can also type in new policy object names or delete names in the Servers list itself. The names you type must be valid names of End Stations or End Station Groups known to the ExtremeWare Enterprise Manager.

The names in the Servers list are separated by semi-colons, following the convention used by Microsoft Outlook.

- c To change the clients to which the policy applies, click the policy object selector button at the right of the Clients field, then select the type of client systems you want to include from the pop-up menu.

Select individual clients and add or remove them from the Selected items list. You can display lists of other types of clients by selecting from the pull-down list in the **Show Type** field.

- 5 Click **Next** to go to the **Application** page, and select the application to which this policy will apply.

- a Click the Application selector button at the right of the **Applications** field. This displays a list of applications known to the Policy System.
- b Select an application and click **OK**. Only one application can be specified for a given policy.

You can also type in a known L4 port by entering the protocol type (TCP or UDP) and a port number.

The form is:

UDP/<port#>

TCP/<port#>

For example: TCP/111

TCP and UDP are the two supported protocol types.

- 6 Click **Next** to go to the **Traffic Treatment** page, and select a Treatment for this policy.
 - a Select a treatment from the pull-down list in the **Treatment** field.
- 7 Click **Next** to go to the **Policy Scoping** page, and specify the scoping for this policy.
 - a To scope this policy for all managed devices, click the **All Managed Devices** button.

- b To select specific Device Groups to which this policy should apply, click the **Specified Device Groups** button.
- To include a device group, select the device group in the **Excluded Device Groups** list and click the **right-arrow button**. The device group will move to the Included Device Groups list.
- To remove device groups from the policy scope, select the Device Group in the **Included Device Groups** list and click the **left-arrow button**. The policy will move to the Excluded Device Groups list.

8 Click Next to go to the **Policy Overlaps** page, and specify the scoping for this policy.

The **Policy Overlaps** list displays a list of policies that overlap or conflict with the new policy based on its definition so far. The **Policy Overlaps** list shows the following information:

- **Overlapping Policy**—the name of the overlapping policy.
- **Relative Precedence**—the precedence of this policy relative to the new policy.
The relative precedence shows the order in which the policies, and the traffic to which they apply, will be handled on the managed network devices on which the policy is configured.
- **Precedence Type**—indicates whether the precedence is Explicit (specifically defined by a user) or Implicit (its precedence is a function of the time at which the policy was created). Precedence type and the rules that determine the precedence between policies is discussed in the next section.

You cannot change the information shown on this page.

If you think the overlap may be the result of an incorrect policy specification, you can use the **Back** button return to the appropriate page, and make the necessary changes.

9 Click Next to go to the **Precedence** page and change the precedence of a policy, if needed.

The precedence lists show how overlapping policies relate to your new policy.

- **Higher Priority Policies** are those which have higher priority (will take precedence) over the new policy.
- **Lower Priority Policies** are those which have lower priority than the new policy (the new policy takes precedence).

If you do not define precedence explicitly among policies, there is an implicit ordering by which precedence is determined. This ordering is done based on two factors:

- The QoS Type of the policy (IP QoS, Source Port QoS, or VLAN QoS).
- The time at which the policy was created.

The precedence based on QoS type overrides all other precedence factors. IP QoS is the highest priority, Source Port QoS is second, and VLAN QoS is the lowest.

Thus, Custom and Client-Server policies will have higher precedence than Source Port policies, which will in turn be higher than a VLAN policy. Since an Application Server policy uses both IP QoS and Source Port QoS depending on the traffic direction, the precedence of an Application Server policy will be different based on the direction of traffic.

If all other precedence variables are equal, the precedence will be determined by the time of creation, with the policy created last having the higher precedence.

- To change the precedence of a listed policy relative to your new policy, select the policy, and click the appropriate directional arrow button to move the policy to the other list.
- To add or remove policies from either of the precedence lists, click the corresponding **Edit** button. You can add other policies, both overlapping and non-overlapping policies, to create precedence relationships with the selected policy. If there are policies in the precedence lists that aren't relevant, you can remove those.

- 10** Click **Next** to go to the **QoS Settings** page to review the potential QoS rules that the policy system expects to generate from the policy definition you've entered.

The QoS rules are the rules that the current definition of the policy expects to generate.

You cannot change the QoS rules displayed under this tab. If the QoS rules are not what you expected, you can use the **Back** button to return to the appropriate page and change the specifications so that the desired QoS rules will be computed.

- 11** Click **Next** to go to the **Policy Definition Complete** page.

You can use the **Back** button to return to a previous page to change components of the policy definition.

Click **Finish** when you are satisfied with your policy definition.

CREATING A POLICY FROM THE NEW MENU

If you are experienced in network policy creation, using the Network QoS Policy view page is a quicker method for creating new policies.

To create a policy using the **New** menu, follow these steps:

- 1 Click the **New** button at the top of the Policy System page, then select **Policy** from the drop-down menu.

A pop-up box appears to let you select the type of policy you want to create (see Figure 8-8).

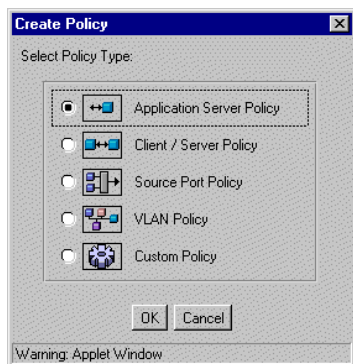


Figure 8-8: Pop-up selection box for Policy type

- 2 Select the type of policy you want to create, then click **OK**.

A Network QoS Policy view appears for the type of Policy you've selected (Figure 8-9).

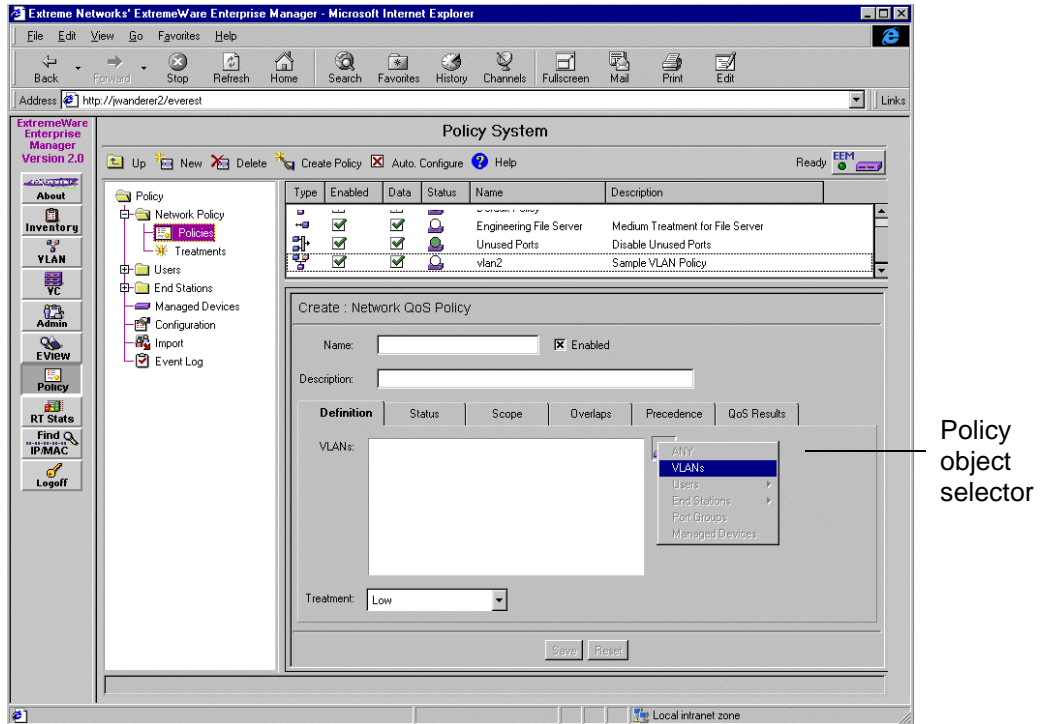


Figure 8-9: Create: Network QoS Policy page for a VLAN policy

This view lets you specify all the components of a network policy by using the various tabs to specify the elements of a policy, as described in the next section.

VIEWING AND MODIFYING NETWORK POLICIES

To view the current network policies defined within the Policy System, click the plus sign next to Network Policy in the Component Tree to display the policy subcomponents, then click **Policy**. This displays the Network QoS Policy view (see Figure 8-10).

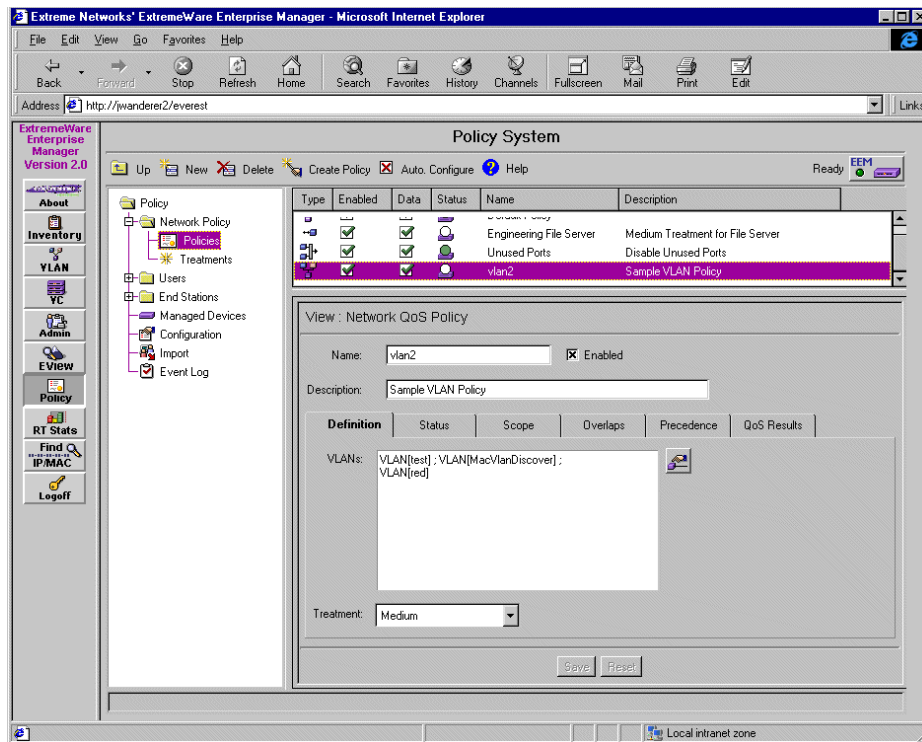




Figure 8-10: Network QoS Policy view for a VLAN policy, Definition tab

The main applet frame has two sections:


- The top section lists all the network policies currently defined in the policy system, with type and status information.
 - **Type** displays an icon showing the type of policy (Application Server, Client/server, Source Port, VLAN, or Custom).
 - **Enabled** indicates whether the policy is enabled. A green check (☒) indicates that the policy is enabled. A red X (☐) indicates that the policy is not enabled.
 - **Data** indicates whether the policy system has sufficient information to compute valid QoS rules for this policy. A green check (☒) indicates that the data is complete. A red X (☐) indicates that additional information is still needed before the policy system can compute QoS rules.
 - **Status** indicates whether the policy has been successfully configured on the target devices.

A small switch with a green light  indicates that the current QoS rules have been configured onto the appropriate network devices.

A small switch with a half-green light  indicates that the current QoS rules have been partially configured onto the appropriate network devices.

A small switch with a white light  indicates that the current QoS rules have not been configured onto the appropriate network devices.

A small switch with a red light  indicates an error condition.

A blue question mark  indicates that the configuration status of the devices is unknown.

- **Name** is the name given to the policy when the policy was created.
- **Description** is the optional description of the policy provided when the policy was created.
- The bottom section shows detailed information about the currently selected network policy.

The Network QoS policy section always displays the name and description of the selected policy, and a check box to indicate whether the policy is enabled.

Beneath this is a series of tabs that show different aspects of the policy definition and status.

THE DEFINITION TAB

Figure 8-10 shows the Definition tab for the selected policy, a VLAN policy. The fields displayed under this tab vary depending on the type of policy displayed.

VLAN POLICY DEFINITION TAB

A VLAN policy generates a set of QoS policy rules that apply the specified treatment (QoS profile) to all the traffic flows from the specified VLANs. Based on the specified VLAN names, the Policy System identifies the switches on which the treatment should be configured.

For the VLAN policy shown in Figure 8-10, the Definition tab shows a list of the VLANs to which this policy applies, and the Treatment that applies to this policy.

- There are two ways to change the list of VLANs to which the policy applies:
 - Click once on the policy object selector button at the right of the VLANs field, then select **VLAN** from the pop-up menu (this will be your only choice).

Select individual VLANs and add or remove them from the Selected items list. When you are finished, click **OK**.

- Type in new VLAN names or delete the names of VLANs in the VLAN list itself. The names you type must be valid names of VLAN known to the ExtremeWare Enterprise Manager.

The name must be in the form:

`VLAN[<vlan_name>]`

It must be preceded by the word VLAN and enclosed in square brackets. Multiple names in the VLAN list are separated by semi-colons, following the convention used by Microsoft Outlook.

For example:

`VLAN[default];VLAN[marketing];VLAN[QA]`

Note: *You cannot modify the Default policy, except to enable or disable it.*

- To change the treatment used for this policy, select a treatment from the pull-down list in the **Treatment** field.
- Clicking **Reset** at any time prior to clicking **Save** will restore the policy definition to those currently in effect for the selected policy.
- Click the **Save** button to save the changes as the new policy definition.

VLAN QoS uses 802.1Q tagging to carry the QoS parameters across VLAN boundaries. In order to allow VLAN policies to be effective end-to-end, you should make sure your switch-to-switch links use tagged ports.

APPLICATION SERVER POLICY DEFINITION TAB

An Application Server Policy generates a set of QoS rules that apply the treatment (QoS profile) to traffic going to the server IP address/Layer 4 port and from the source port to which the server is connected on an Extreme switch. You specify the application (which translates to a well-known Layer 4 port) and server when you create the policy. The Policy System determines the source port.

An Application Server policy affects traffic in both directions: however, it actually generates two different uni-directional QoS implementations. The policy is implemented as Source Port QoS on the traffic outbound from server, and as IP QoS for the traffic going to the server.

For an Application Server policy (Figure 8-11) the Definition tab shows a list of the servers and the application to which this policy applies, and the Treatment that is used by this policy.

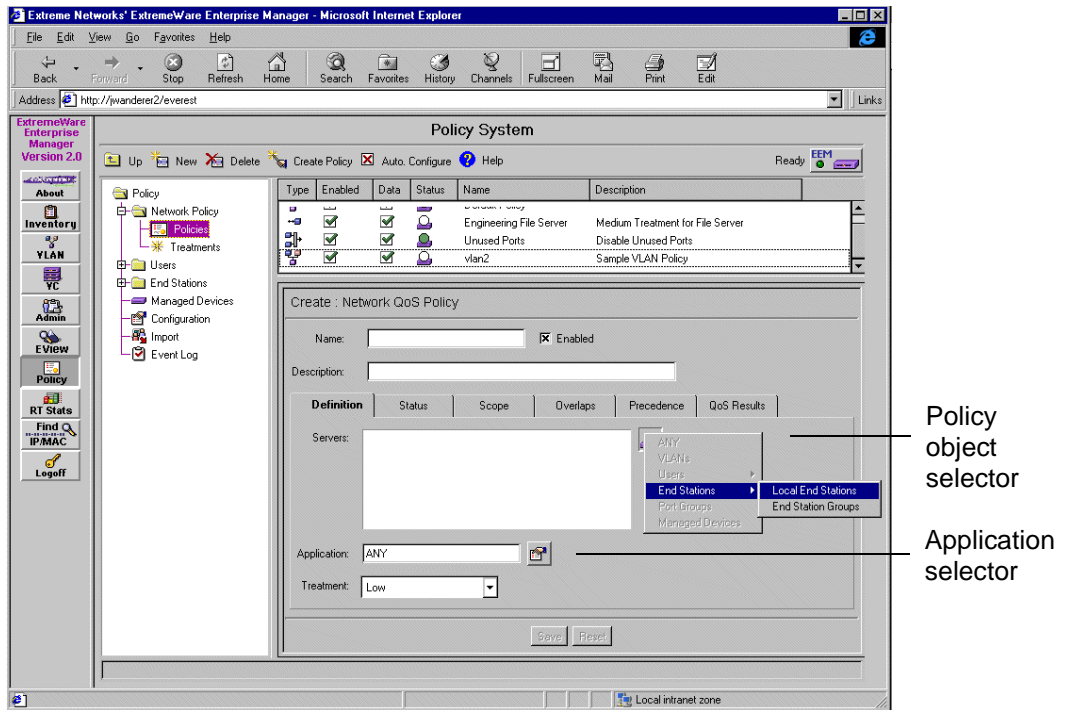


Figure 8-11: Network QoS Policy view for an Application server policy, Definition tab

- There are two ways to change the list of servers to which the policy applies:
 - Click the policy object selector button at the right of the Servers field, then select **End Stations**, and either **Local End Stations** or **End Station Groups** from the pop-up menu. A dialog box appears.

Select individual end stations or end station groups and add or remove them from the Selected items list. You can display either the Local End Stations list or the End Station Groups list by selecting from the pull-down list in the **Show Type** field.

When you have finished, click **OK**.

- You can type in new End Station or End Station Group names or delete names in the Servers list itself. The names you type must be valid names already known to the Extremeware Enterprise Manager.

The names in the Servers list are separated by semi-colons, following the convention used by Microsoft Outlook.

- To change the application, click the Application selector button at the right of the Application field. This displays a list of applications known to the Policy system. Select an application and click **OK**. The Policy System maps the application name to the well-known Layer 4 port associated with the application. A policy can apply to only one application—you must create a separate policy for each application you want to control.

The Application choice **ANY** tells the Policy System to apply the defined treatment to ALL traffic from the specified servers. In this case, the IP address only (without a Layer 4 port designation) is used as the endpoint.

You can also type in the name of any known Layer 4 port by entering the protocol type (TCP or UDP) and a port number. The form is:

UDP/<port#>

TCP/<port#>

For example: TCP/111

TCP and UDP are the two supported protocol types.

- To change the treatment used for this policy, select a treatment from the pull-down list in the **Treatment** field.
- Clicking **Reset** at any time prior to clicking **Save** will restore the policy definition to those currently in effect for the selected policy.
- Click the **Save** button to save the changes as the new policy definition.

CLIENT/SERVER POLICY DEFINITION TAB

A Client/Server policy maps a QoS treatment to traffic going between a server and specific clients. You specify the both sets of endpoints (clients and server) between which the traffic will travel. The server endpoint can also include an application (translated to a Layer 4 port) or it can be a host (indicated by the application choice “ANY,” translated to an IP address only). The Policy System determines the switches that are affected by this policy. The policy you specify is implemented as IP QoS in both directions between the client and server. Although not shown in the diagram, you can specify multiple servers as well as multiple clients.

Note: Specifying a large number of servers and clients can result in a very large number of traffic flows. The diagram below (Figure 8-12) shows the number of traffic flows generated for a simple example of two servers and two clients. For “n” servers and “m” clients, the number of traffic flows affected by the policy will be $m*n$.

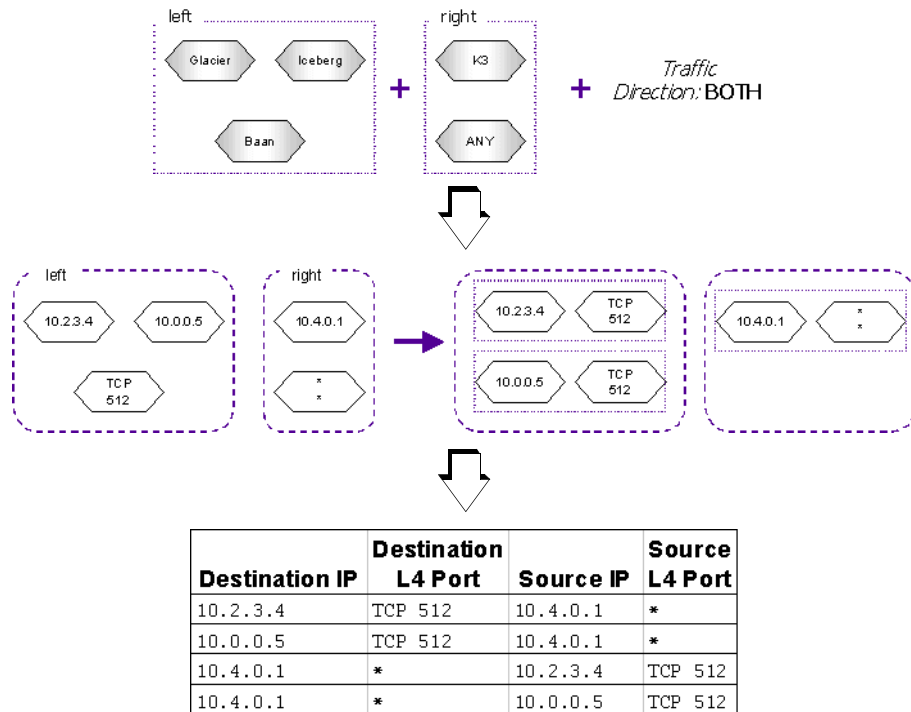


Figure 8-12: Translation of a Client/Server policy definition into traffic flows

For a Client/Server policy, the Definition tab shows a list of the servers, clients, and the application to which this policy applies, and the Treatment used by this policy (see Figure 8-13).

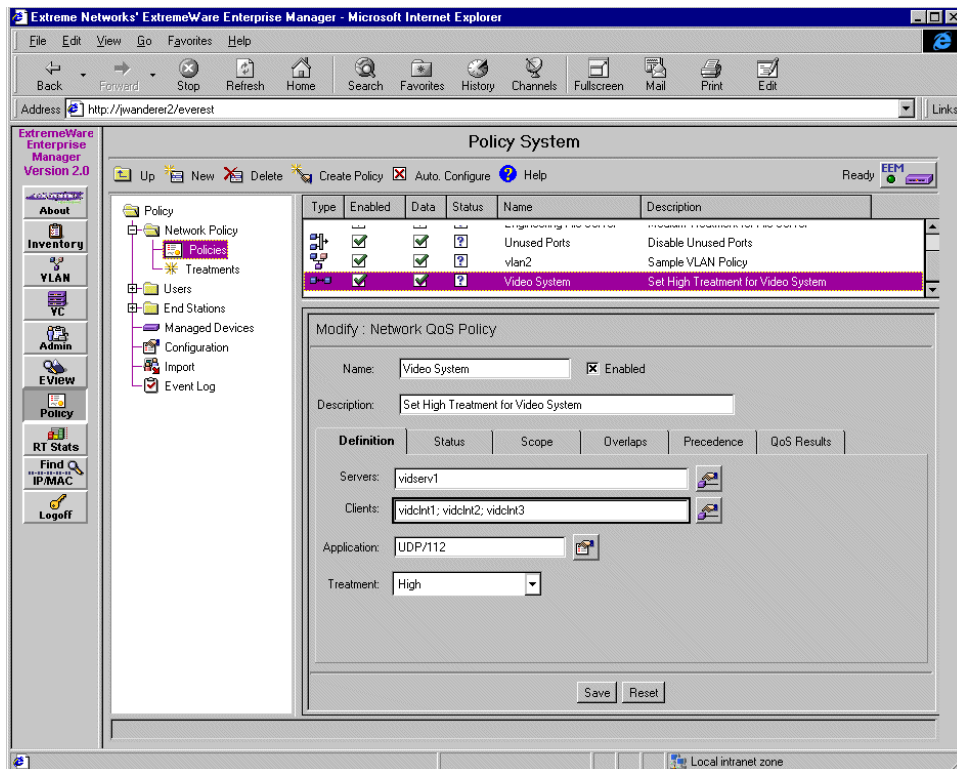


Figure 8-13: Network QoS Policy view for a Client/Server policy, Definition tab

- To change the list of servers to which the policy applies:
 - Click the policy object selector button at the right of the **Servers** field.

You can specify the servers by using any of the available high-level objects: Users, User groups, End Stations, End Station Groups, or Devices. The Policy system will take policy objects you designate, along with an application (L4 port) if you designate one, and translate these into a set of IP addresses that will specify the server-side endstations for this policy.

Select individual users, user groups, end stations, end station groups, or devices and add or remove them from the Selected items list in the dialog box that

appears. You can display lists of other policy objects by selecting from the drop-down list in the **Show Type** field. When you have finished, click **OK**.

- You can also type in new policy object names or delete names in the Servers field itself. The names you type must be valid names of policy objects already known to the Extremeware Enterprise Manager.

The names in the Servers field are separated by semi-colons, following the convention used by Microsoft Outlook.

- To change the clients to which the policy applies:
 - Click the policy object selector button at the right of the Clients field, then select the type of client systems you want to include from the pop-up menu.

You can specify clients using any of the available high-level objects: Users, User Groups, End Stations, End Station Groups, or Devices. The Policy system translates these into a set of IP addresses that will specify the client-side endstations for this policy.

Select individual clients and add or remove them from the Selected items list in the dialog box that appears. You can display lists of other types of clients by selecting from the pull-down list in the **Show Type** field.

- As with the Servers field, you can also type in new policy object names or delete names in the Clients field itself. The names you type must be valid names of policy objects already known to the Extremeware Enterprise Manager, and must be separated by semi-colons.

- To change the Application, click the Application selector button at the right of the Applications field. This displays a list of applications known to the Policy system.

Select an application and click **OK**. A policy can apply to only one application.

The Application choice **ANY** tells the Policy System to apply the defined treatment to ALL traffic from the specified servers. In this case, the IP address only (without a Layer 4 port designation) is used as the endpoint.

You can also type in the name of any known L4 port by entering the protocol type (TCP or UDP) and a port number. The form is:

UDP/<port#>

TCP/<port#>

For example: **TCP/111**

TCP and UDP are the two supported protocol types.

- To change the treatment used for this policy, select a treatment from the drop-down list in the **Treatment** field.

- Clicking **Reset** at any time prior to clicking **Save** will restore the policy definition to those currently in effect for the selected policy.
- Click the **Save** button to save the changes as the new policy definition.

SOURCE PORT POLICY DEFINITION TAB

A Source Port policy maps a QoS treatment to traffic from a specific port on an Extreme switch. You specify the ports from which the traffic will originate. As shown in Figure 8-3, a source port policy is uni-directional, and implements Source Port QoS on the traffic from the specified source port.

For a Source Port policy (see Figure 8-14) the Definition tab shows a list of the physical switch ports to which this policy applies, and the Treatment that used by this policy.

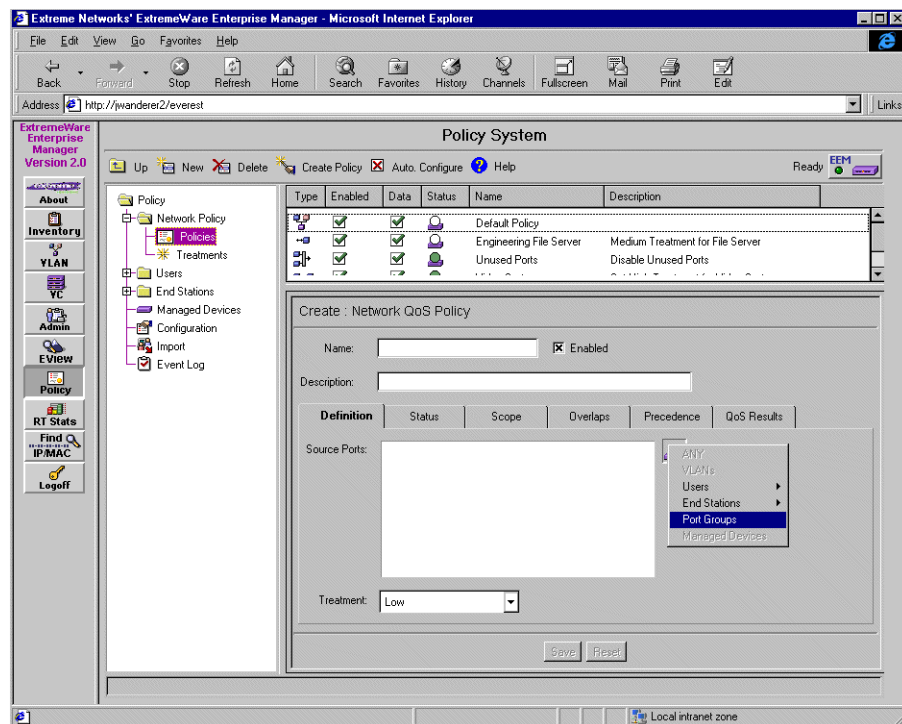


Figure 8-14: Network QoS Policy view for a Source Port policy, Definition tab

- To change the list of source ports to which the policy applies:

- Click the policy object selector button at the right of the Source Ports field, then select the type of policy object for which you want to specify the source port pop-up menu. Source Ports are specified (implicitly) for users or end stations, and explicitly using port sets.

Select source port specifications and add or remove them from the Selected items list. You can display lists of other types of policy objects by selecting from the pull-down list in the **Show Type** field.

When you have finished, click **OK**.

- You can also type in new switch port names or delete the port names in the Source Port list itself.

The name must be in the form:

```
<switchname>[<port#>,<port#range>,...]
```

The port number must be preceded by the switch name, and the list of ports must be enclosed in square brackets. Multiple switches are separated by semi-colons, following the convention used by Microsoft Outlook.

For example:

```
Summit24[1];Summit48[3-5,29,41]
```

- To change the treatment used for this policy, select a treatment from the pull-down list in the **Treatment** field.
- Clicking **Reset** at any time prior to clicking **Save** will restore the policy definition to those currently in effect for the selected policy.
- Click the **Save** button to save the changes as the new policy definition.

Source Port QoS depend on 802.1Q tagging to carry the QoS parameters across switch boundaries. In order to allow Source Port policies to be effective end-to-end, you should make sure your switch-to-switch links use tagged ports.

CUSTOM POLICY DEFINITION TAB

A Custom policy lets you define all the parameters of the policy without any predefinition. A custom policy is always implemented as IP QoS.

For a Custom policy the Definition tab, as shown in Figure 8-15, shows the endpoints, applications and direction that defines the traffic pattern to which this policy applies, and the treatment that is used by this policy.

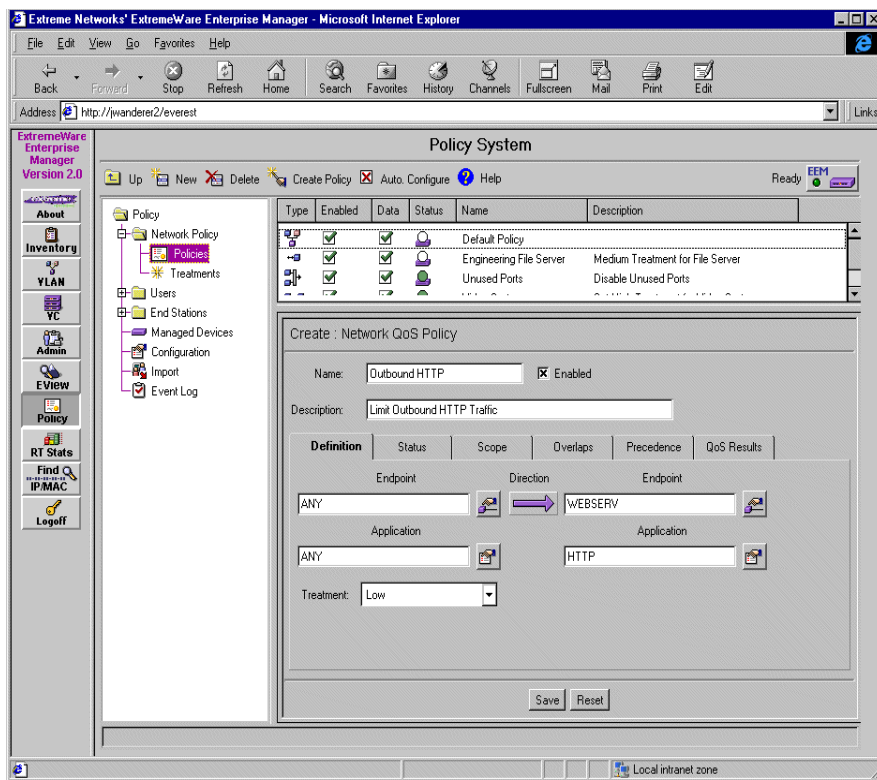


Figure 8-15: Network QoS Policy view for a Custom policy, Definition tab

- To add or change the endpoints to which the policy applies:
 - Click the policy object selector button at the right of the either Endpoint field, then select the type of endpoint from the pop-up menu.

Select individual endpoints and add or remove them from the Selected items list. You can display lists of other types of policy objects by selecting from the pull-down list in the **Show Type** field.

When you have finished, click **OK**.

- You can enter new policy object names, or delete names in the Endpoint field itself. The names must be valid names of policy objects already known to the Extremeware Enterprise Manager. You can also enter IP addresses or subnet addresses directly into this field.

The names in the Endpoint field are separated by semi-colons, following the convention used by Microsoft Outlook.

- To use a subnet as an endpoint, enter the subnet designation in dotted quad notation. For example, you can enter a subnet in the form 10.0.0.* or 10.0.0.0/20.

There are some restrictions on the use of subnets in a Custom policy:

- A non-multi-cast subnet can be used only as the destination, and only in a uni-directional policies.
- A multi-cast subnet can be used as either the source or the destination of the traffic in a uni-directional policy.
- To change the traffic direction, click the box with the arrow between the two Endpoint fields. The arrow is three-way toggle between forward, reverse, and bi-directional.
- To change the application associated with an endpoint (or set of endpoints), click the Application selector button at the right of either **Application** field. This displays a list of applications known to the Policy System.

Select an application and click **OK**. You can specify one application for either endpoint.

You can also type in the name of any known L4 port by entering the protocol type (TCP or UDP) and a port number (for example: **TCP/111**). The form is:

UDP/<port#>

TCP/<port#>

TCP and UDP are the two supported protocol types.

- To change the treatment used for this policy, select a treatment from the pull-down list in the **Treatment** field.
- Clicking **Reset** at any time prior to clicking **Save** will restore the policy definition to those currently in effect for the selected policy.
- Click the **Save** button to save the changes as the new policy definition.

THE STATUS TAB

Figure 8-16 shows the Status tab. This tab displays the selected policy's readiness and configuration status.

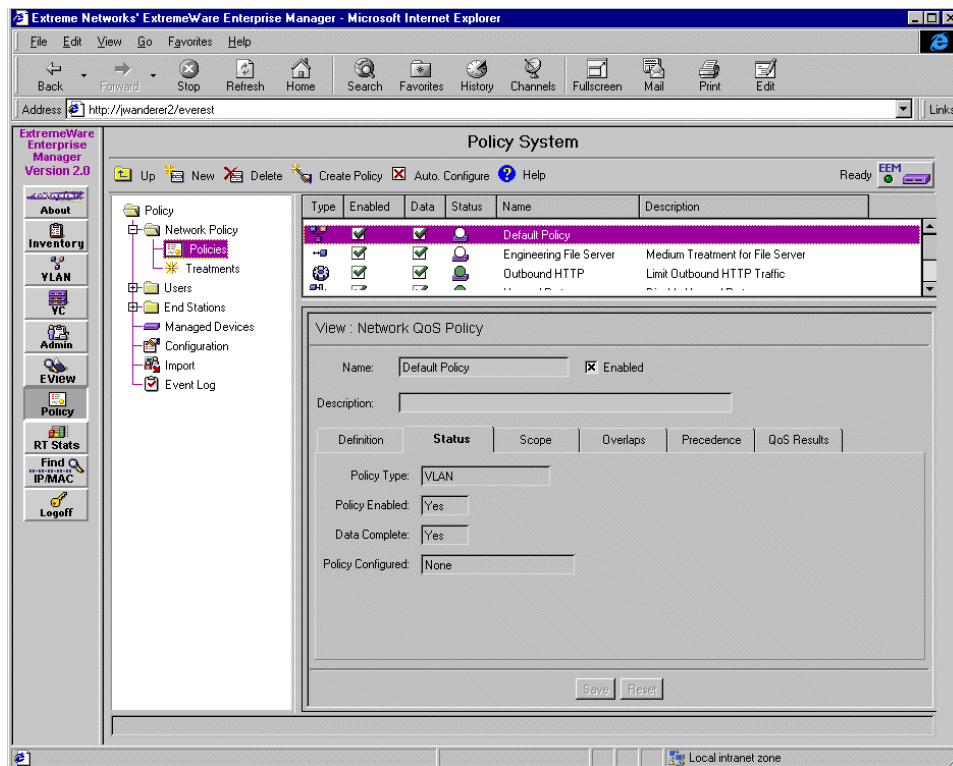


Figure 8-16: Network QoS Policy view for a VLAN policy, Status tab

The Status tab displays the following fields:

- The Policy type.
- Whether the policy is enabled.
- Whether the policy data is complete (whether the Policy system has sufficient information about the end stations or user policy objects, to compute valid QoS rules for this policy).
- Whether this policy has been successfully configured onto the devices within its scope.

This screen is a status only display; no modifications can be made to these fields. The Save and Reset buttons are disabled.

Note: If the Policy Configured field shows the message “Error: Too many rules” this means you need to reduce the number of endpoints that your policy specifies.

THE SCOPE TAB

Figure 8-17 shows the Scope tab for the selected policy. The Scope tab shows the range of network devices to which the policy can be applied.

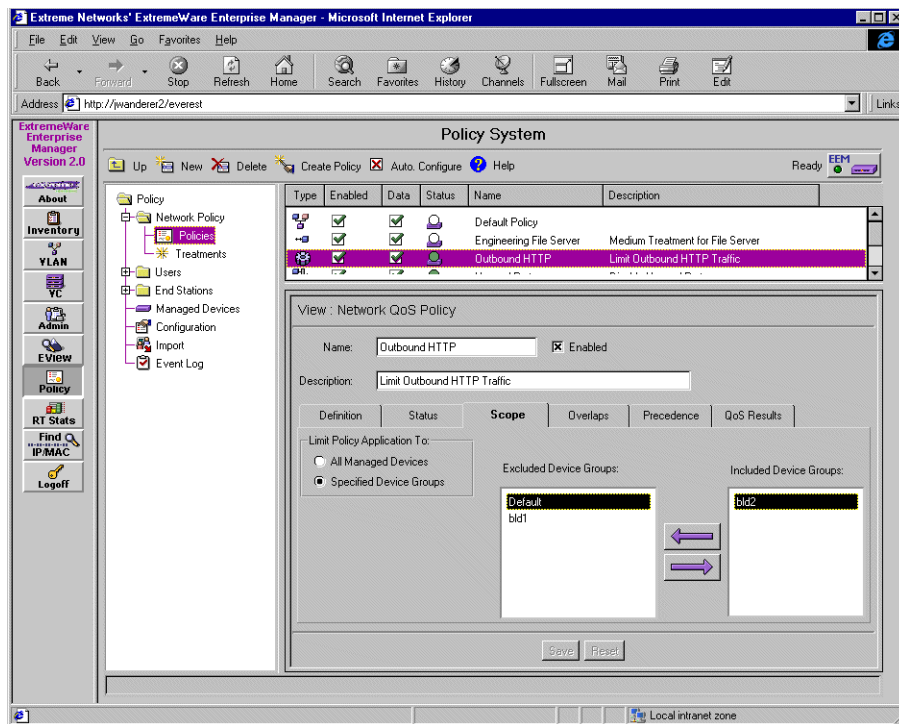


Figure 8-17: Network QoS Policy view for a VLAN policy, Scope tab

The Scope tab displays the following information:

- Whether the policy applies to All Managed Devices, or whether it is limited to Specified Device Groups.

When **All Managed Devices** is selected, this policy automatically applies to any newly-added devices and any new device groups created after the policy has been defined.

- If **Specific Device Groups** is selected, the display shows which groups are included and which are excluded.
 - To include an excluded policy, select the policy in the Excluded Device Groups list and click the **right-arrow** button. The policy moves to the Included Device Groups list.
 - To remove device groups from the policy scope, select the policy in the Included Device Groups list and click the **left-arrow** button. The policy moves to the Excluded Device Groups list.

Note: *The scope of the default VLAN policy cannot be changed.*

- Clicking **Reset** at any time prior to clicking **Save** will restore the policy definition to those currently in effect for the selected policy.
- Click the **Save** button to save the changes as the new policy definition.

THE OVERLAPS TAB

Figure 8-18 shows the Overlaps tab for the selected policy.

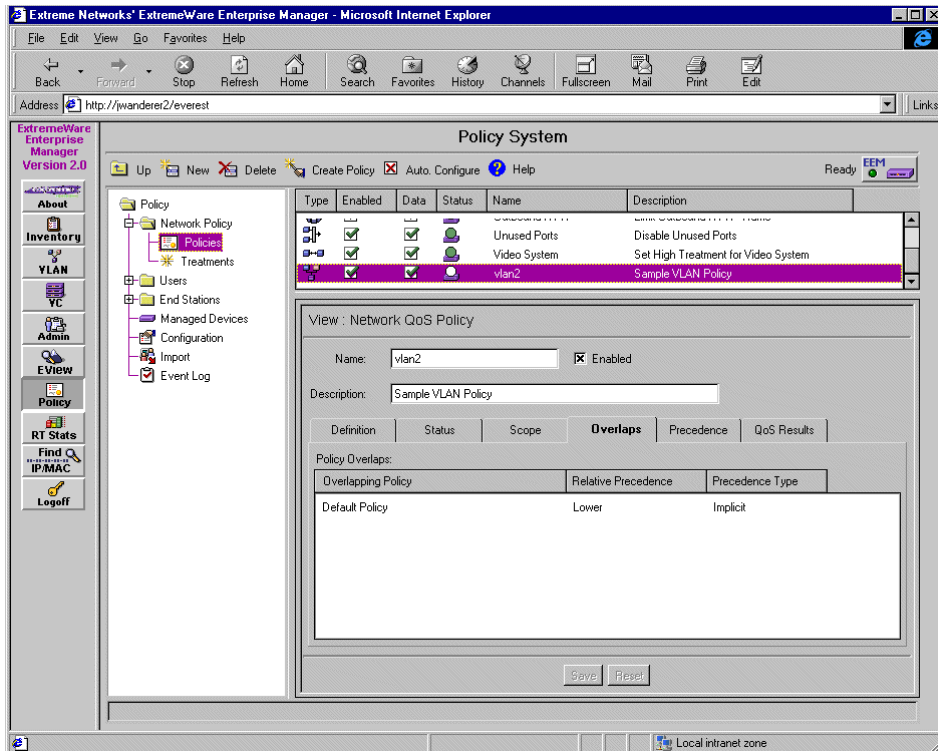


Figure 8-18: Network QoS Policy view for a VLAN policy, Overlaps tab

The Overlaps tab displays a list of policies that overlap or conflict with the selected policy. The Policy Overlaps list shows the following information:

- Overlapping Policy—the name of the overlapping policy.
- Relative Precedence—the precedence of this policy relative to the other policies in the list.

The relative precedence shows the order in which the policies will be configured on the managed network devices to which it applies.

- Precedence Type—indicates whether the precedence is Explicit (specifically defined by a user) or Implicit (its precedence is a function of its QoS type and the time at

which it was created). Precedence type and the rules that determine the precedence between policies in discussed in the next section.

You cannot change the information shown under this tab—the Save and Reset buttons are disabled.

To change the precedence of a policy, click the Precedence tab and make changes there. If you think the overlap may be the result of an incorrect policy specification, you can return to the appropriate tab and make the necessary changes. You can do the same for any other policy by selecting that policy in the list display at the upper half of the screen.

THE PRECEDENCE TAB

This tab lets you assign an “explicit” precedence for a specific policy, within the basic precedence relationships determined by the QoS implementation type of the policy.

Precedence based on QoS type overrides all other precedence factors. IP QoS gets the highest priority, Source Port QoS is second, and VLAN QoS is given the lowest priority. Traffic with higher priority is forwarded by the switch before traffic of lower priority

Thus, Custom and Client-Server policies have higher priority than Source Port policy, which is in turn higher than a VLAN policy. Since an Application Server policy uses both IP QoS and Source Port QoS depending on the traffic direction, the precedence of an Application Server policy will be different based on the direction of the traffic.

If all other precedence variables are equal, and you do not define the precedence explicitly, then precedence is determined by the time of creation, with the policy created last having the higher precedence.

Figure 8-19 shows the Precedence tab for a selected policy.

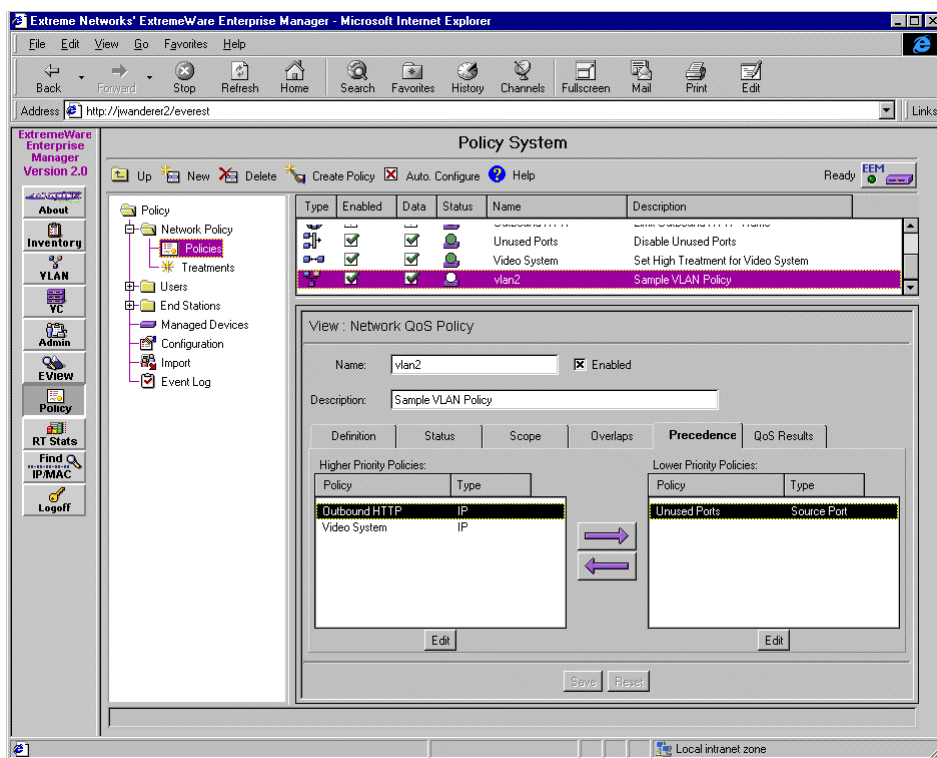


Figure 8-19: Network QoS Policy view for a VLAN policy, Precedence tab

The Precedence tab displays the following information:

- The precedence lists show how overlapping policies relate to the selected policy.
 - Higher Priority Policies are those which have higher priority (take precedence) over the currently selected policy. Traffic to which these policies apply will be forwarded before traffic of lower priority.
 - Lower Priority Policies are those which have lower priority than the currently selected policy (the selected policy takes precedence).
- To change the precedence of a listed policy relative to the selected policy, select the policy, and click the appropriate directional arrow button to move the policy to the other list.
- To add or remove policies from either of the precedence lists, click the corresponding **Edit** button. You can add other policies, both overlapping and non-overlapping policies, to create precedence relationships with the selected policy. If there are

policies in the precedence lists that aren't relevant, you can remove them. You can also add and remove other network QoS policies from a precedence relationship with the selected policy.

Click **OK** to return to the Precedence tab.

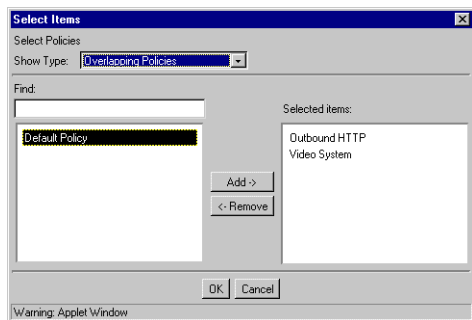


Figure 8-20: Edit: Select Policies pop-up window

- Clicking **Reset** at any time prior to clicking **Save** will restore the precedence settings to those currently in effect relative to the selected policy.
- Click the **Save** button to save the changes for the affected policies.

THE QoS RESULTS TAB

Figure 8-21 shows the QoS Results tab. This shows the QoS rules that have been computed from the selected policy.

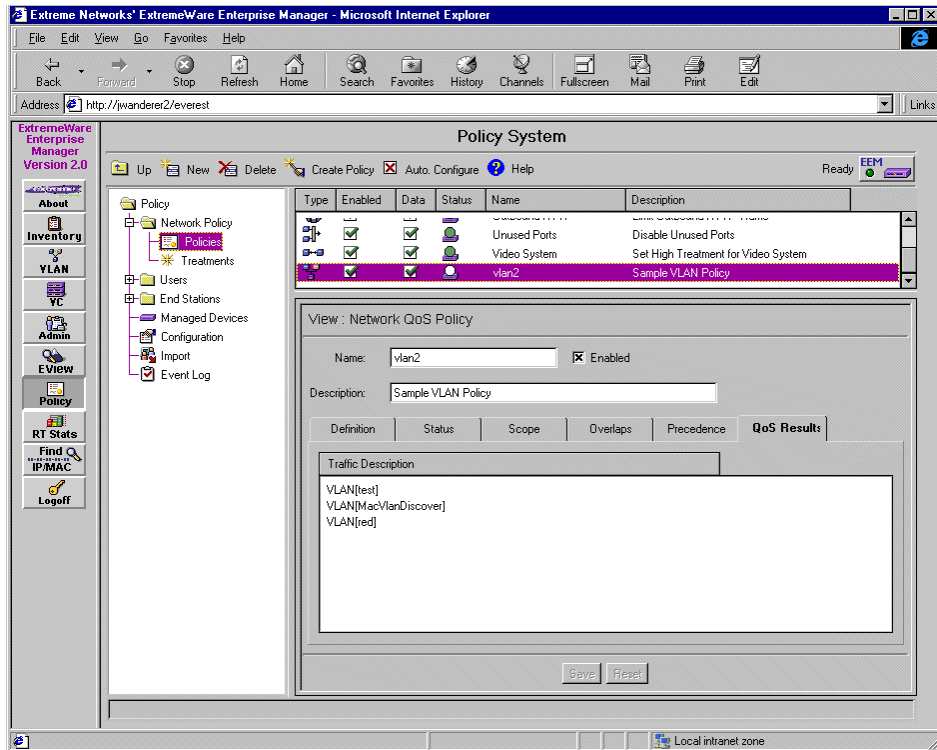


Figure 8-21: Network QoS Policy view for a VLAN policy, QoS Results tab

The QoS rules are the rules that the current definition of the policy expects to generate. Note that these may not correspond exactly to the computed QoS rules because the computed rules take into account the intersection of multiple policies.

You cannot change the QoS rules displayed under this tab. The Save and Reset buttons are disabled. If the QoS rules are not correct, you should return to the appropriate tab and change the specifications so that the correct QoS rules will be computed.

VIEWING AND MODIFYING NETWORK QoS TREATMENTS

To view the current QoS treatments defined within the Policy System, click the plus sign next to Network Policy to display the policy subcomponents, then click **Treatment**. This displays the Network QoS Treatment view (see Figure 8-22).

The main applet frame has two sections:

- The top section lists all the treatments currently defined in the policy system.
 - **Name** is the name of the treatment provided when the treatment was created.
 - **Description** is the optional description of the treatment provided when it was created.
- The bottom section shows detailed information about the currently selected treatment:
 - The name and description of the selected treatment.
 - The scope of the treatment: device groups on which the treatment will be configured. You can have a different set of treatment definitions for different device groups.
 - The treatment values (minimum and maximum bandwidth, and priority) for this treatment.

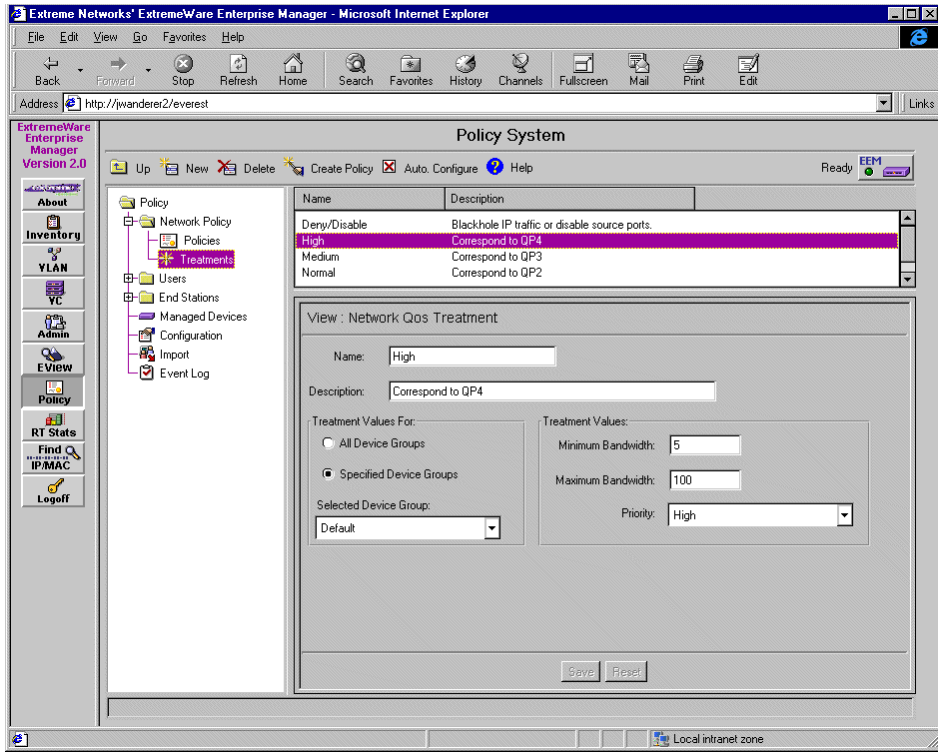


Figure 8-22: Network QoS Treatment view

There are five treatments: four quality treatments (corresponding to QP1-QP4) and Deny/Disable (corresponding to Blackhole IP traffic or disabling source ports). The default definitions for QoS treatments are shown in Table 8-1.

Table 8-1: Default QoS Treatments

QoS Treatment Name	Description	Priority	Min Bandwidth	Max Bandwidth
Deny/Disable	Blackhole/disable source ports	None	0	0
Low	Corresponds to QP4	Low	0%	100%
Normal	Corresponds to QP3	Normal	0%	100%
Medium	Corresponds to QP2	Medium	0%	100%
High	Corresponds to QP1	High	0%	100%

QoS treatments cannot be added or deleted. You can change the names and descriptions of all five treatments, and you can change the priority and bandwidths of the four quality treatments.

Treatments can be scoped, so that you can have different treatment parameters for each device group.

- To change the scope for the treatments, click **All Device Groups** or **Selected Device Groups**. If the treatment is to be scoped for specific device groups, you can select those groups from the pull-down list in the **Selected Device Group** field, or type the Device Group names into the field (separated by semi-colons).
- To change the minimum bandwidth for the treatment, type a value into the **Minimum Bandwidth** field. The value must be between 0 and 90, and less than or equal to the value you plan to use for maximum bandwidth.
Note: *The sum of all minimum bandwidth cannot be greater than 90%.*
- To change the maximum bandwidth for the treatment, type a value into the **Maximum Bandwidth** field. The value must be between 0 and 100, and greater than or equal to the minimum bandwidth specified in the previous field.
- To change the priority, select a priority (Low, Normal, Medium, or High) from the pull-down list in the **Priority** field.

ADDING OR MODIFYING LOCAL USERS

- 1 To add a new user, click **New** at the top of the Policy System page, then select **User** from the pull-down list.

To modify an existing End Station, select **Local Users** under the **Users** entry in the Component Tree.

Either method will display the **Network User** page as shown in Figure 8-23.

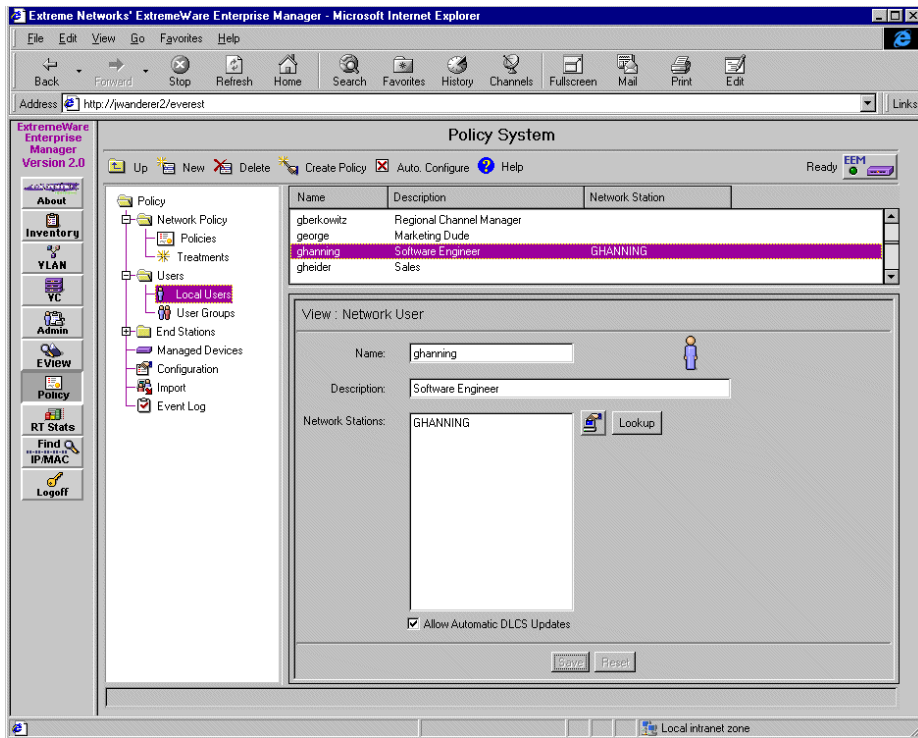



Figure 8-23: The Network User View

- 2 To add a new user, type the user name in the **Name** field, and an optional description in the **Description** field.
- 3 If DLCS is running in your network devices, you can click **Lookup**, and the Enterprise Manager will use DLCS to try to find any end stations where this user is logged in. It will enter them for you in the Network Stations field.
If DLCS is not running, or if the Enterprise Manager cannot find the user, you can enter network stations manually in the Network Station field.
- 4 Click the selector box to the right of the **Network Stations** field to display a list of the end stations known to the Enterprise Manager. Select end station names from this list and use the **Add ->** button to add them to the selected list. Use **Remove ->** to remove names from this list. When you are finished, click **OK**.
- 5 Click **Save** to save the additions or changes.

A check  in the **Allow Automatic DLCS Updates** box means that the policy system will get network station information for the user from the switch's DLCS feature.

This will be done automatically every time the QoS policies are re-configured. If auto-configuration is turned on, changes to DLCS mappings in the switch (due to a user logging in or logging out) will trigger a re-configuration.

The default for **Allow Automatic DLCS Updates** is *on* (box is checked).

Note: *DLCS must be enabled on the switch before the policy system can make use of the feature. DLCS cannot be enabled through the Enterprise Manager.*

ADDING OR MODIFYING USER GROUPS

- 1 To create a new User Group, click **New** at the top of the Policy System page, then select **User Group** from the pull-down list.

To modify an existing User Group, select **User Groups** under the **Users** entry in the Component Tree.

Either method will display the **Local Group – Users** page as shown in Figure 8-24.

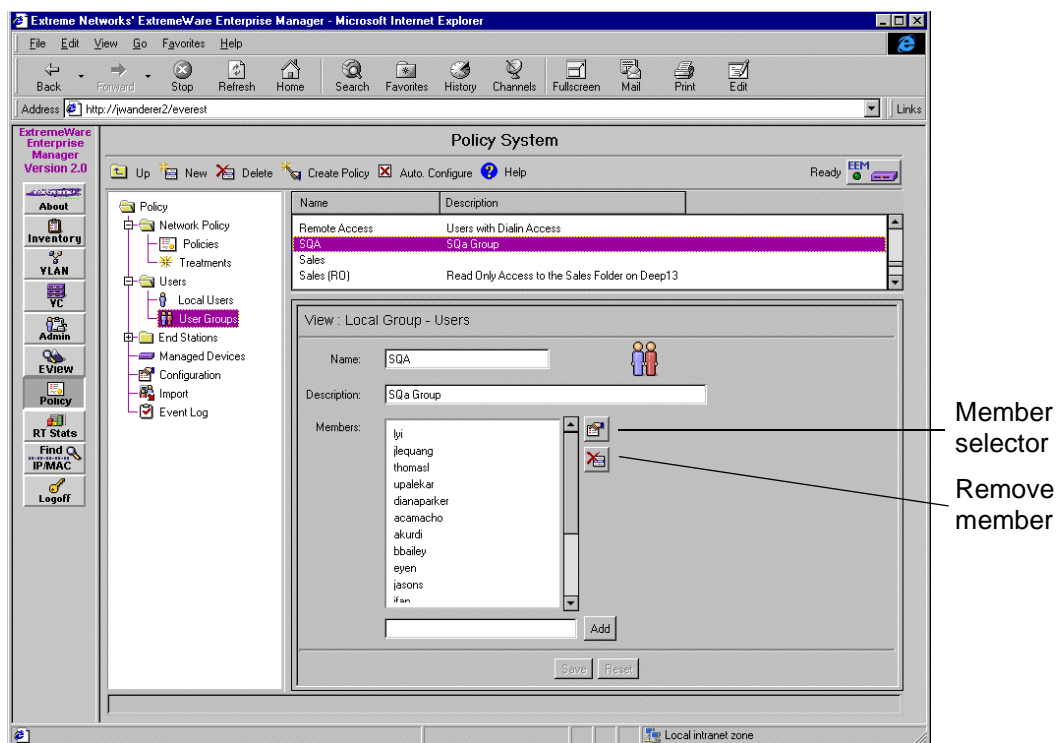


Figure 8-24: The Local Group – Users view

- 2 To add a new User Group, type the group name in the **Name** field, and an optional description in the **Description** field.
- 3 Click the selector box to the right of the **Members** field to display a list of the users known to the Enterprise Manager. Select user names from this list and use the **Add ->** button to add them to the **Selected items** list. Use **Remove ->** to remove names from this list. When you are finished, click **OK**.

- 4 You can also add members by typing a user name in the **Add** field at the bottom of the screen. Type the name and click **Add** to add it to the members list.
- 5 To remove members from the User Group, select one or more names in the Members list and click the Remove members button (just below the selector button to the right of the Members list) to remove them from the list.
- 6 Click **Save** to save the additions or changes.

ADDING OR MODIFYING END STATIONS

An **End Station** is a named host defined as a policy object for use in policy definitions. An End Station name is dynamically translated into an IP address, switch and port when QoS rules are computed from a policy definition for configuration onto network devices.

The easiest way to create End Station objects is to import them from an NT Domain Controller or Solaris NIS maps (see “Importing Data from NT Domains or Solaris NIS” on page 8-57).

However, there may be situations where you must either add an End Station manually, or change or add information for an existing End Station. Do this as follows:

- 1 To create a new End Station, click **New** at the top of the Policy System page, then select **End Station** from the pull-down list.
To modify an existing End Station, select **Local End Stations** under the **End Stations** entry in the Component Tree.
Either method will display the **Local End Stations** page as shown in Figure 8-25.

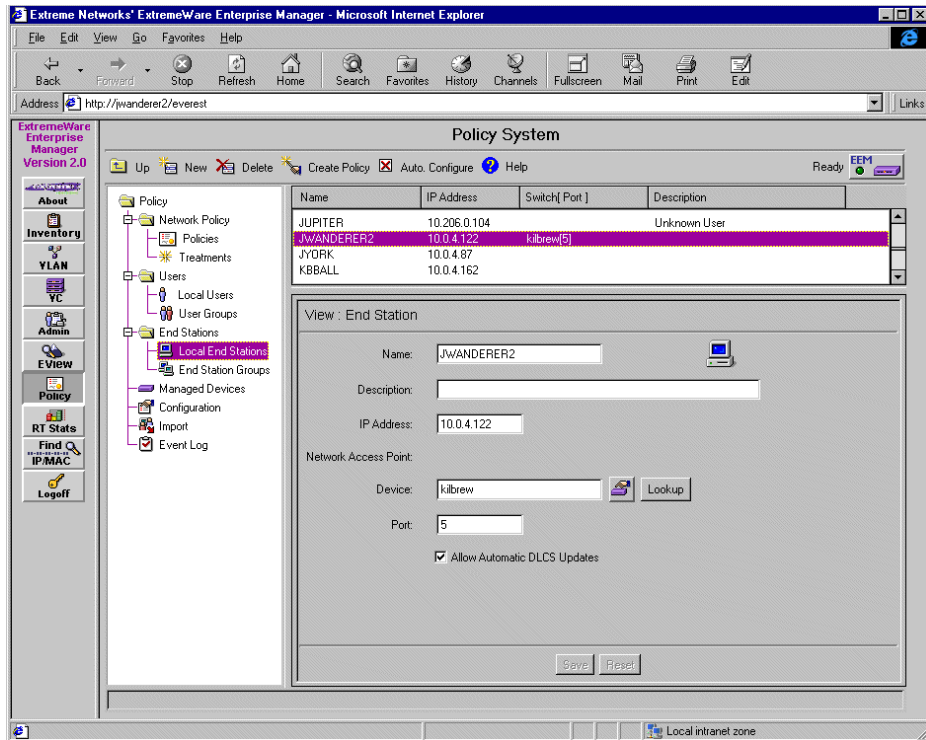



Figure 8-25: The End Station view.

- 2 To add a new end station, type the host name in the **Name** field, and an optional description in the **Description** field.
- 3 If DLCS is running in your network devices, you can click **Lookup**, and the Enterprise Manager will use DLCS to try to find the IP Address, switch device, and port associated with the host name you entered. It will enter them for you into the appropriate fields.
If DLCS is not running or cannot find the host, then type the host IP Address into the **IP Address** field.
- 4 Click the Device selector box to the right of the **Device** field to list the Access Devices known to the Enterprise Manager. Select the appropriate device from this list and click **OK**.
- 5 Enter the port number into the Port field.
- 6 Click **Save** to save the additions or changes.

A check  in the **Allow Automatic DLCS Updates** box means that the policy system will get IP address and switch/port information for the end station from the switch's DLCS feature.

This will be done automatically every time the QoS policies are re-configured. If auto-configuration is turned on, then changes to DLCS mappings in the switch (due to an end station booting up) will trigger a re-configuration.

The default for **Allow Automatic DLCS Updates** is *on* (box is checked).

Note: *DLCS must be enabled on the switch before the policy system can make use of the feature. DLCS cannot be enabled through the Enterprise Manager.*

ADDING OR MODIFYING END STATION GROUPS

End Station Groups are named groups of hosts that you can use as policy objects in policy definitions. They are dynamically translated into IP addresses, switches and ports when QoS rules are computed from the policy definitions for configuration onto network devices.

- 1 To create a new End Station Group, click **New** at the top of the Policy System page, then select **End Station Group** from the pull-down list.

To modify an existing End Station Group, select **End Station Groups** under the **End Stations** entry in the Component Tree.

Either method will display the **End Station Groups** page as shown in Figure 8-26.

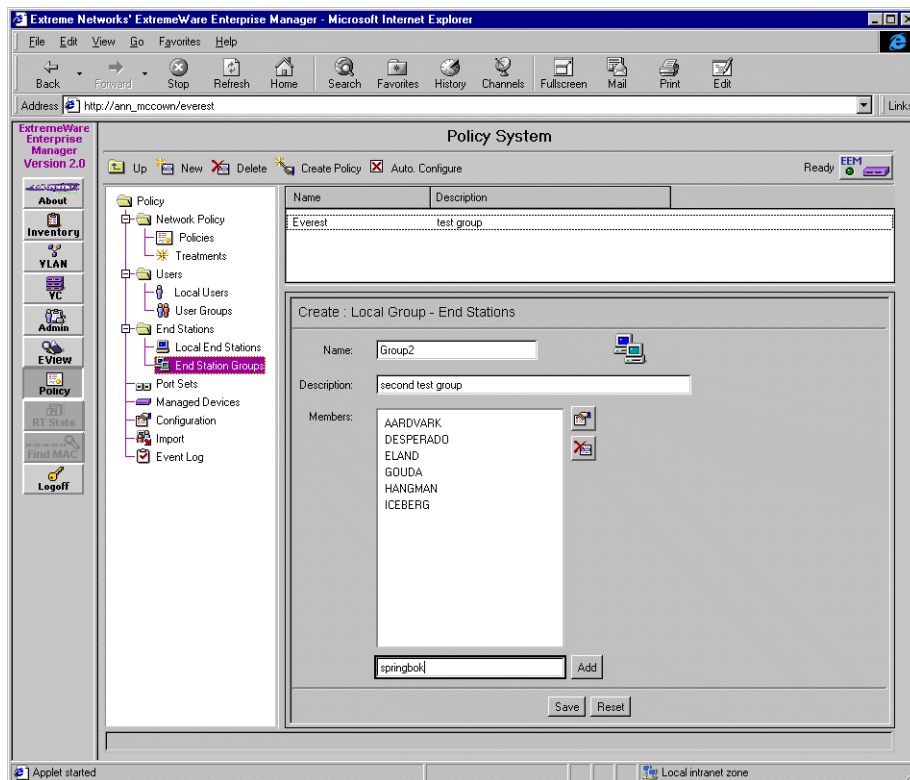


Figure 8-26: The End Station Group view.

- 2 To add a new End Station Group, type the group name into the **Name** field, and a description (optional) into the **Description** field.
- 3 Click the selector box to the right of the **Members** field to display a list of the end stations known to the Enterprise Manager. Select end station names from this list and use the **Add** -> button to add them to the selected list. Use **Remove** -> to remove names from this list. When you are finished, click **OK**.
- 4 You can also add members by typing a host name into the **Add** field at the bottom of the screen. Type the name and click **Add** to add it to the members list.
- 5 To remove members from the End Station Group, select one or more hosts in the Members list and click the Remove button (just below the selector button to the right of the Members list) to remove them from the list.
- 6 Click **Save** to save the additions or changes.

DISPLAYING MANAGED DEVICE STATUS

Select **Managed Devices** in the Component Tree to display a list of all the managed devices known to the Enterprise Manager.

Selecting a device in the Devices list displays the name, description and IP address of the device (see Figure 8-27). You cannot change the device information displayed on this page—use the Modify Devices function in the Inventory Manager to modify device configuration information.

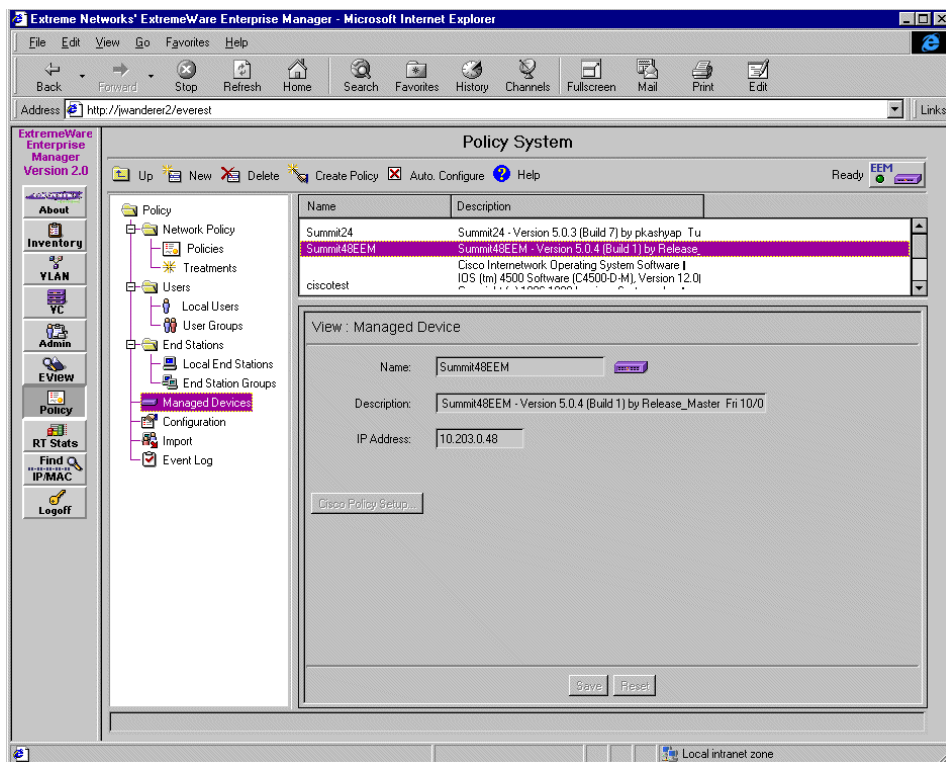


Figure 8-27: The Managed Devices View

CISCO DEVICE POLICY SETUP

You can set up policy for a Cisco device running Cisco IOS 11.2 or later.

- 1 Select a Cisco Device in the Devices list, then click the **Cisco Policy Setup** button. This button will not be available unless a Cisco device is selected.

This displays the Cisco Device Policy Setup window as shown in Figure 8-28.

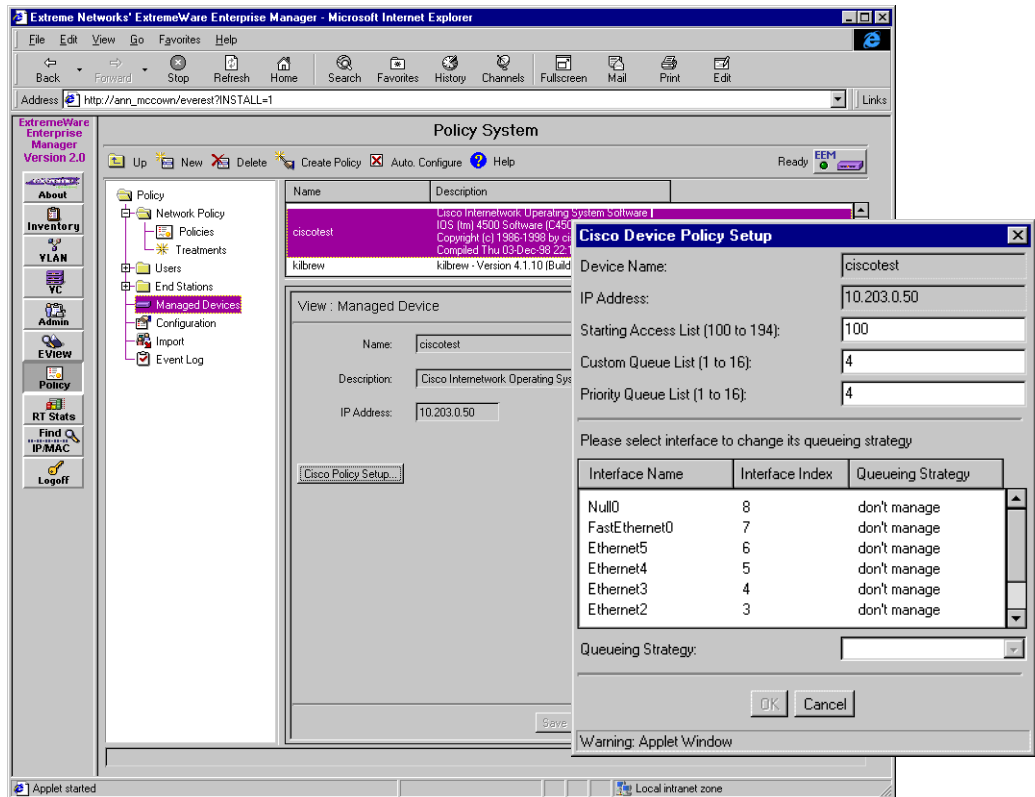


Figure 8-28: Setting Cisco Device Policy

The values displayed initially are either those read from the switch, or else are default values determined by ExtremeWare Enterprise Manager.

- 2 To change the Access List Start, Custom Queue List, or Priority Queue List, type a new value in the appropriate field. The values you can use for these are as follows:

- **Access Start List:** ExtremeWare Enterprise Manager uses six consecutive access lists to specify traffic on a Cisco device. You can specify the starting access list, and Enterprise Manager will use that list plus the following five. For example, if you specify 100, then Enterprise Manager will use access lists 100 through 105.
You can specify a starting access list between 100 and 194. The default, if no access list is yet configured on the device, is -1.
 - **Custom Queue List:** You must specify a custom queue list for Enterprise Manager to use to apply policies that do bandwidth control. You can specify a custom queue list from 1 to 16. The default, if no queue list is yet configured on the device, is -1.
 - **Priority Queue List:** You must specify a priority queue list for Enterprise Manager to use to apply policies that do priority control. You can specify a priority queue list from 1 to 16. The default, if no queue list is yet configured on the device, is -1.
- 3** For each interface to which ExtremeWare Enterprise Manager will apply policies, select the interface in the Interface list, and select a queueing strategy from the drop down list in the Queueing Strategy field.
- Select **Custom Queue List** to bind the custom queue you have selected to the interface, so ExtremeWare Enterprise Manager can do bandwidth control on this interface.
 - Select **Priority Queue List** to bind the priority queue you have selected to the interface, so ExtremeWare Enterprise Manager can do priority control on this interface.
 - Select **Don't Manage** if ExtremeWare Enterprise Manager should not manage this interface. This is the default strategy.
- 4** Click **OK** when you have completed your policy setup.

Once you have specified the access lists, and the custom and priority queue lists for ExtremeWare Enterprise Manager, Enterprise Manager will assume complete control of these resources. They will override any other settings configured outside Enterprise Manager for these resources. The parameters are stored in the ExtremeWare Enterprise Manager database, and are also written into the Cisco device login banner. If the same device is added again or “sync”ed to the Enterprise Manager database, these parameters will be read from the device during the synchronization process.

CONFIGURING QoS POLICIES

If Automatic Configuration is turned on ☒ every change you make within the ExtremeWare Enterprise Manager will trigger an immediate re-computation and reconfiguration of the QoS policies on your network. Configuration changes on a device managed by ExtremeWare Enterprise Manager, or a user login or end station reboot when DLCS is enabled, also trigger a recomputation and reconfiguration of QoS policies.

If auto-configuration is turned off ☐ you must explicitly perform the configuration process.

Click **Configuration** in the Component Tree to display the Configuration page (see Figure 8-29).

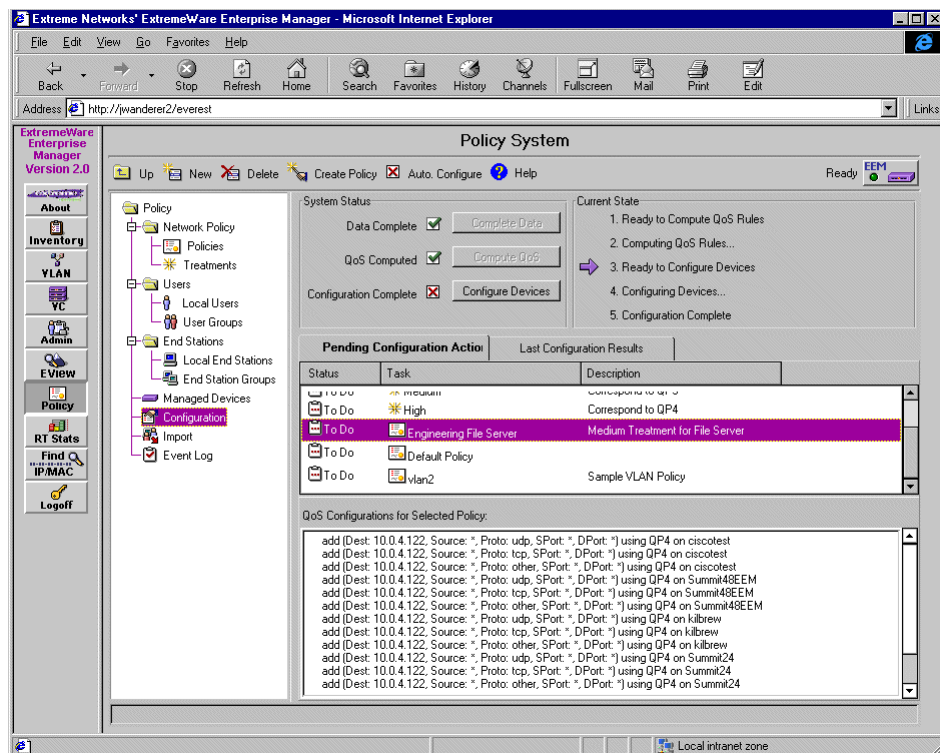




Figure 8-29: The Policy System Configuration view.



SYSTEM STATUS

The System Status block indicates the status of the policy configuration process.


- **Data Complete** indicates whether the policy system has sufficient information about a host (end station) or user policy object, to compute valid QoS rules. For example, you might not have entered an IP address for a host. A green check  indicates that the data is complete. If DLCS is enabled, the Data Complete status will indicate that the data is complete, even if information has not yet been obtained.


A red X  indicates that additional information is still needed before the policy system can compute QoS rules.

Note: *If you have **Allow Automatic DLCS Updates** checked for a user (or end station), then data will always be considered Data Complete, because the policy system will assume that it will get the required parameters from DLCS on the switch.*

- **QoS Computed** indicates whether the QoS rules have been successfully computed. A green check  indicates that the rules have been computed successfully.
A red X  indicates that the QoS rules have not been computed since policy definition changes were made.

Click **Compute QoS** to compute a new set of QoS rules.

- **Configuration Complete** indicates whether the QoS rules have been successfully configured onto the appropriate network devices. A green check  indicates that the current QoS rules have been configured onto the appropriate network devices.

A blue question mark  indicates that the configuration status of the devices is unknown. You must compute the QoS rules to see a configuration status.


Click **Configure Devices** to initiate the configuration process. If the QoS rules have not been computed, clicking **Configure Devices** will first cause those rules to be computed, and then do the device configuration.

CURRENT STATE

The Current State block shows you the state of the policy system. The purple arrow indicates the current state.

- **Ready to Compute QoS Rules** indicates that policy definition changes have been made that require computation of new or modified QoS rules.

To start rule computation, click **Compute QoS** in the System Status block.

- **Computing QoS Rules** indicates that computation is under way. While this is occurring, the Policy System State icon in the upper right corner of the Policy System page will indicate Busy. 
- **Ready to Configure Devices** indicates that a set of QoS rules has been computed incorporating all current policy definition changes. The rules are now ready to be configured on the appropriate devices.

To start the configuration process, click **Configure Devices** in the System Status block.

- **Configuring Devices...** indicates that the policy system is in the process of configuring the network devices with the new QoS rules. While this is occurring, the Policy System State icon in the upper right corner of the Policy System page will indicate Busy.
- **Configuration Complete** indicates that the configuration process has finished. The Policy System will maintain this state until a change in a policy definition requires a recomputation and reconfiguration. At that point, assuming auto-configuration is off, the state will change to **Ready to Compute QoS Rules**.

IMPORTING DATA FROM NT DOMAINS OR SOLARIS NIS

You can import information on users, user groups, and local end stations from either a Windows NT Domain Controller, or a NIS server in a Solaris environment. The type of system on which you are running the ExtremeWare Enterprise Manager server will determine where the policy system looks to find this data.

For Windows NT, the ExtremeWare Enterprise Manager Server must be running with the appropriate user permissions in order to import users from the Domain Controller. If you cannot import users due to permissions, see your system administrator or see the installation instructions in Chapter 2 for details on setting these permissions when you install the ExtremeWare Enterprise Manager Server.

Select **Import** from the Component Tree to display the Import page (see Figure 8-30).

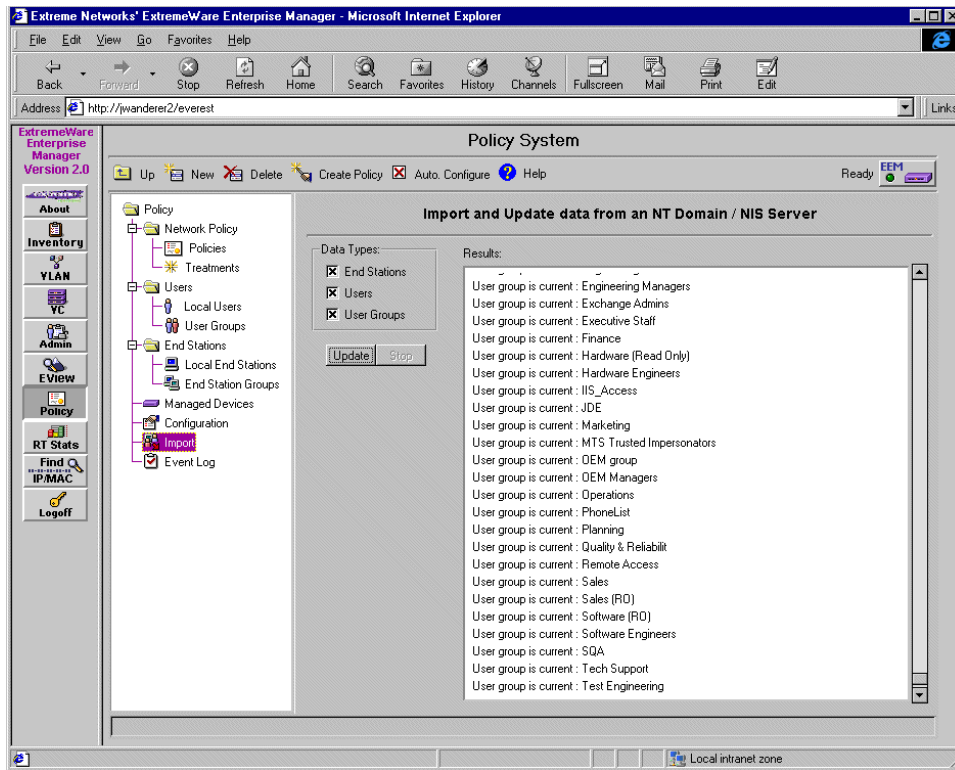


Figure 8-30: The Import Data view

- Select the types of data you want to import in the **Data Types** box, then click **Update** to start the import. If you want to stop the process before it is finished, click **Stop**.

Import will update existing data if it has changed, as well as add new users and end stations.

DISPLAYING THE EVENT LOG

The Event Log displays the configuration events that have been performed on any of the managed devices since the ExtremeWare Enterprise Manager client was last started, up to a limit of 25 Kbytes of messages.

Select **Event Log** from the Component Tree to display the Event Log page (see Figure 8-31).

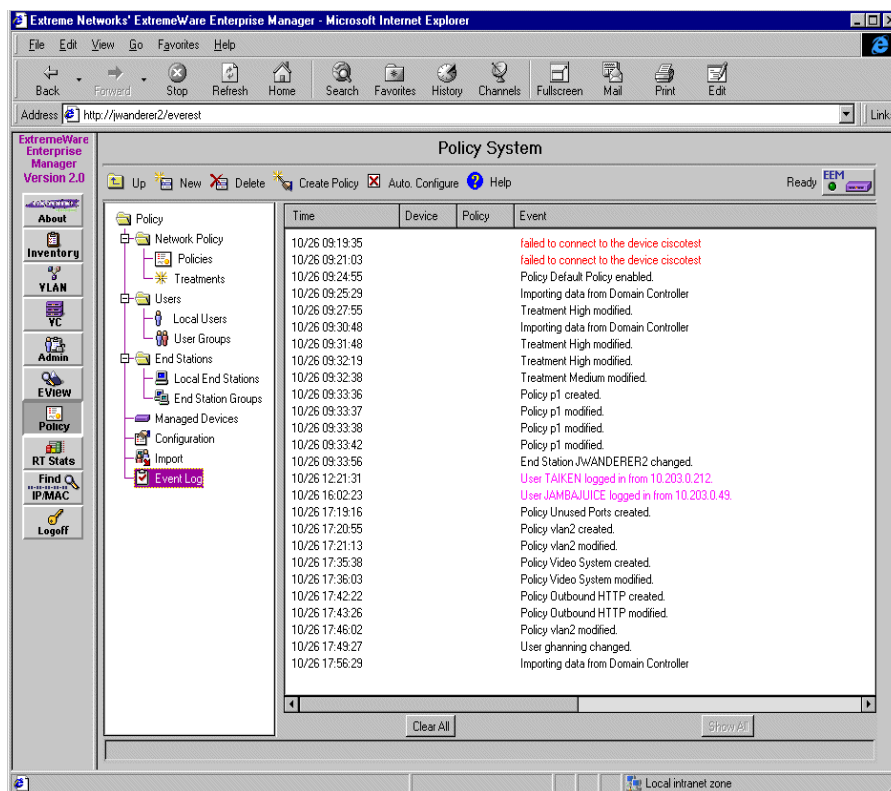


Figure 8-31: The Event Log

The **Clear All** button clears the Event Log *display* only—the event data remains in the log file. Click **Show All** to restore the display of the full Event Log

9

Managing Virtual Chassis Stacks

This chapter describes how to use the Virtual Chassis Stack Manager for:

- Displaying a Virtual Chassis stack.
- Updating the Virtual Chassis stack topology.
- Creating a Virtual Chassis stack.
- Editing a Virtual Chassis stack.
- Deleting a Virtual Chassis stack.

OVERVIEW OF VIRTUAL CHASSIS STACKS

The Summit Virtual Chassis is a high performance, low cost external backplane that connects up to eight stacked or distributed Summit switches into one cohesive system. A Virtual Chassis (VC) stack is a configuration of one to four Summit Virtual Chassis and up to eight connected Summit switches.

Note: See the Summit Virtual Chassis Design and Installation Guide for a discussion and examples of Summit Virtual Chassis stack configurations.

The Virtual Chassis Stack Manager applet of the ExtremeWare Enterprise Manager lets you identify virtual stack configurations, as well as manually create, modify, and delete Virtual Chassis stack topology representations in the Enterprise Manager database. Managing stack topologies through the VC Stack Manager does not affect the actual switch configurations. Only port configurations can be changed on the switch through the VC Stack Manager.

ExtremeWare Enterprise Manager manages Virtual Chassis stacks as aggregated entities. The Enterprise Manager uses an SNMP identification process to recognize virtual stacks and their components, based on the known Extreme switches. This information is stored in the Enterprise Manager database.

The Enterprise Manager can automatically identify single stacks and single parallel stacks. However, it does not support identification of combined virtual chassis stack configurations, and identifies such configurations as multiple stacks. Using the Virtual Chassis Stack Manager you can change the stack configuration representations to reflect actual single and parallel managed stack configurations. You can also create stack representations manually, independent of the stack identification process.

Users with Administrator or Manager access can create, modify, and delete VC stacks and refresh the stack topology identification. Users with Monitor access can view the VC stack configuration topology and the details about individual components.

IDENTIFYING VIRTUAL CHASSIS STACK TOPOLOGIES

To create or identify Virtual Chassis stacks, several prerequisites must be met:

- All switches that are to be members of the VC stacks must be included in the ExtremeWare Enterprise database. If not, the VC stack will be incomplete.
 - You must add switches to the switch inventory using the Add Switch function in the Inventory Manager.
 - The newly added switches will appear as Orphan Switches in the VC stack topology display.
- The appropriate ports on each switch must be properly configured in SummitLink mode. They must also be configured for load sharing as appropriate.
 - This assumes that the switches are cabled correctly as VC stack members.
 - Configure the switch ports by selecting the switch in the Orphan Switch list in the VC Stack Manager Component Tree, and clicking **Config** to bring up the Configure Ports in VC Stack dialog box. See “Configuring Virtual Chassis Stack Ports” for details.
 - Reboot the switches.
- Once the ports are configured, you can use the **Identify** function to identify VC stacks.

Each Summit device uses the Extreme Discovery Protocol (EDP) to identify all neighboring Summits connected via a Summit Virtual Chassis. The Virtual Chassis Stack Manager uses SNMP to collect this information about VC connections from each managed Summit switch in the ExtremeWare Enterprise Manager database. Using this information, the VC stack Manager constructs a collection of VC stacks and leftover Summits (orphan Summits) and VCs (orphan VCs).

This process can identify many, but not all stack topologies. There are two basic types of VC stack configurations: single stacks and parallel stacks. Within the Enterprise Manager, a Summit switch or a VC can belong to only one VC stack. Thus, if a Summit switch has connections to multiple VCs in separate stacks, the Enterprise Manager may not be able to place the switch correctly.

You can edit the VC stack configurations to reflect the actual managed stack configurations in your network. You can also create stack representations manually, independent of the stack identification process.

Once you have created or edited the VC stacks manually, the representations in the Enterprise Manager database will not change unless you change them manually, or unless you explicitly request a re-identification using the **Identify** function (see “Identifying the Virtual Chassis Stack Topology”).

DISPLAYING THE VIRTUAL CHASSIS STACK TOPOLOGY

To display the current Virtual Chassis (VC) stack topology, click the **VC** button in the ExtremeWare Enterprise Manager Navigation toolbar. The Virtual Chassis Stack Manager window is displayed, as shown in Figure 9-1.

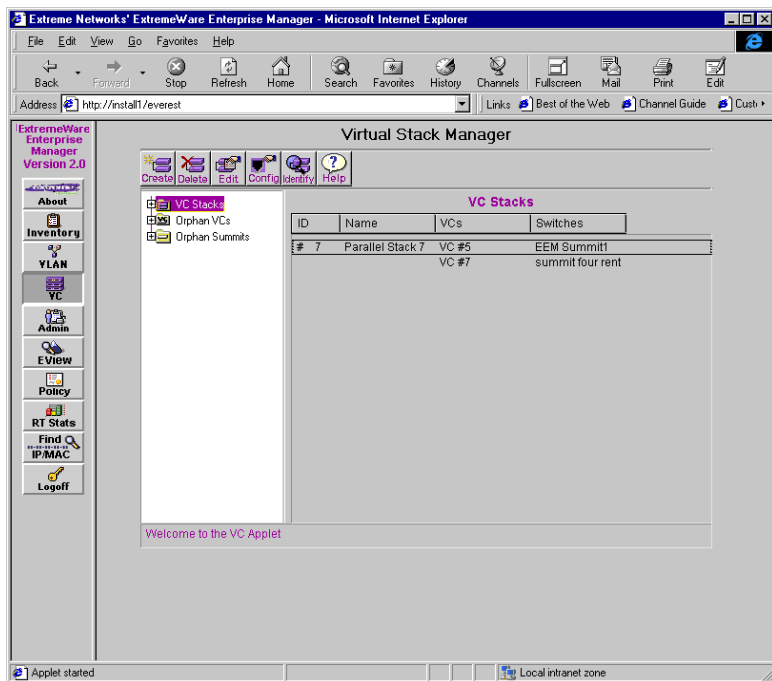


Figure 9-1: Virtual Chassis Stack Manager display of known Virtual Chassis stacks

As with the other ExtremeWare Enterprise Manager applets, the Component Tree is displayed in the left-hand panel. Detailed information about a selected component is displayed in the right-hand panel.

In Figure 9-1, the top-level component, VC Stacks, is selected. The detail shows the stack configurations known to the Enterprise Manager database.

- **VC Stacks** lists each Virtual Chassis stack that has been detected by the Enterprise Manager, or that has been created manually by the user. It also shows all switches and VCs detected as components of the stacks.
- **Orphan VCs** are any Virtual Chassis that do not appear to be components of any VC stack, as detected by Enterprise Manager. A VC can appear to be an orphan because:
 - The Enterprise Manager cannot determine the stack to which it belongs.
 - It has been newly identified through EDP since the last stack identification was done through the VC Stack Manager.

- **Orphan Summits** are any Summit switches that do not appear to be components of any VC stack. They do not appear to have any port connections to a Virtual Chassis. A Summit switch can be classified as an orphan because:
 - The Enterprise Manager cannot determine the stack to which it belongs.
 - It was added using the Inventory Manager after the most recent identification was completed.
 - It does not have any VC connections.

Five buttons are provided at the top of the Virtual Chassis Stack Manager page. These are, from left to right:

- **Create**—Lets you create a Virtual Chassis Stack.
- **Delete**—Lets you delete a Virtual Chassis Stack.
- **Edit**—Lets you add ports to and remove ports from a Virtual Chassis Stack.
- **Configure**—Lets you configure the Gigabit Ethernet ports on a switch to be SummitLink ports, and to participate in load sharing.
- **Identify**— Identifies all the Virtual Chassis stacks that the ExtremeWare Enterprise Manager can recognize.

You must have Administrator or Manager access to use these functions.

DISPLAYING A VIRTUAL CHASSIS STACK

You can display a graphical representation of a VC stack by selecting the stack in the Component Tree. Figure 9-2 shows the components of the VC stack named “Simple Stack.” It displays all the VCs and Summit switches in the stack, as known to the ExtremeWare Enterprise Manager database, and the ports that interconnect the VCs and switches.

When you invoke the Virtual Stack Manager applet for the first time, all the Summit switches in the Enterprise Manager database are listed as orphans, and no Virtual Chassis are displayed. You must identify the VC stacks before you can display them. See “Identifying the Virtual Chassis Stack Topology” for details.

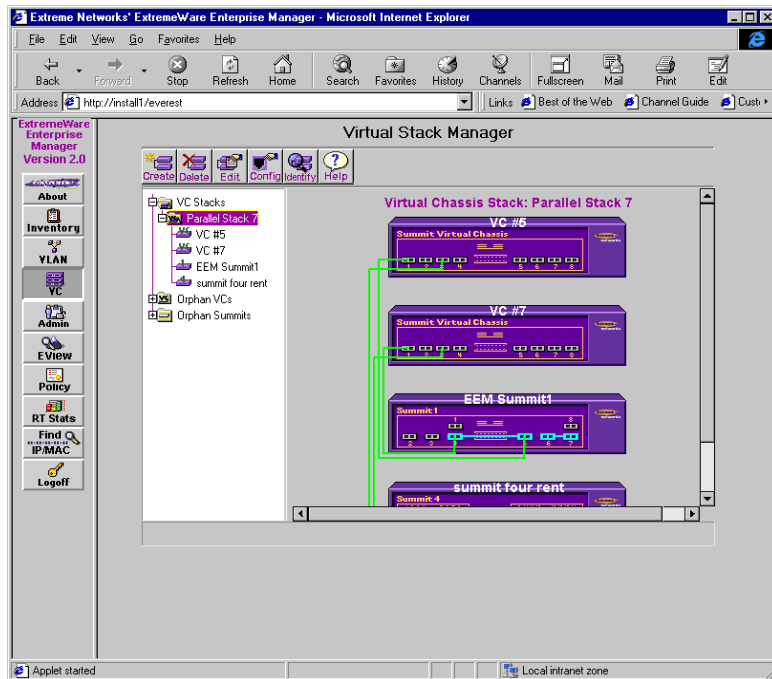


Figure 9-2: Details of an individual Virtual Chassis Stack

The following functions are available from this page:

- Click on a Virtual Chassis or a switch to highlight the connections from that VC or switch.
- Click on a connection to highlight the individual connection.
- Double-click on a switch to invoke ExtremeWare Vista for the switch. This launches a Web browser window and displays the ExtremeWare Vista Login page.

For information on how to use ExtremeWare Vista, refer to “Using ExtremeWare Vista” in the *Summit Switch Installation and User Guide*.

DISPLAYING A VC STACK COMPONENT

You can display details about an individual component of a VC stack by selecting the component in the Component Tree. Figure 9-3 shows the display for an individual Virtual Chassis, showing the ports used.

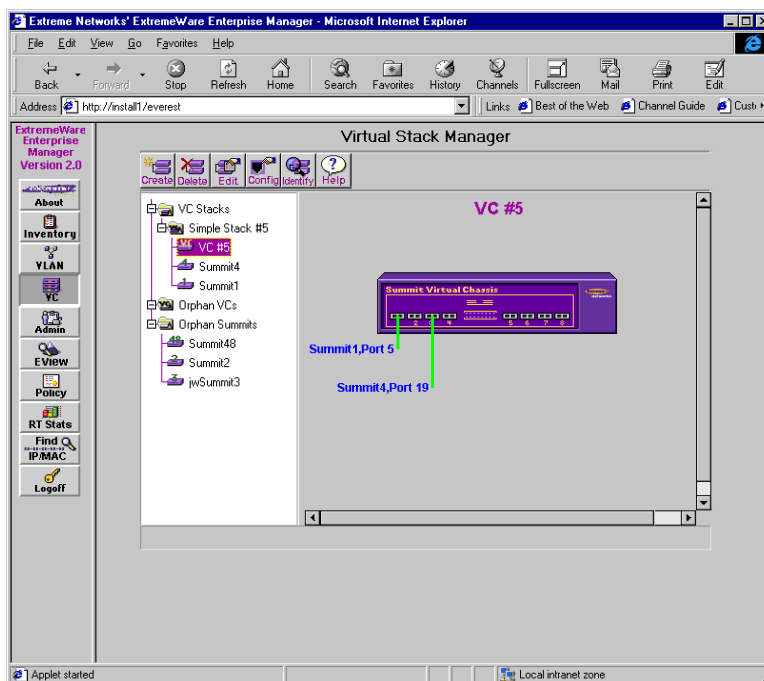


Figure 9-3: Detail view of a Virtual Chassis component of a VC stack

DISPLAYING ORPHAN VCS

Orphan VCs are any Virtual Chassis that do not appear to be members of a VC stack, as detected by ExtremeWare Enterprise Manager.

- To display a list of the VCs, select Orphan VCs in the Component Tree, as shown in Figure 9-4.

A Virtual Chassis may appear to be an orphan if:

- It was removed from a VC Stack using the Enterprise Manager.
- It once was part of a stack and was known to the Enterprise Manager database, but its physical connections have subsequently been removed.

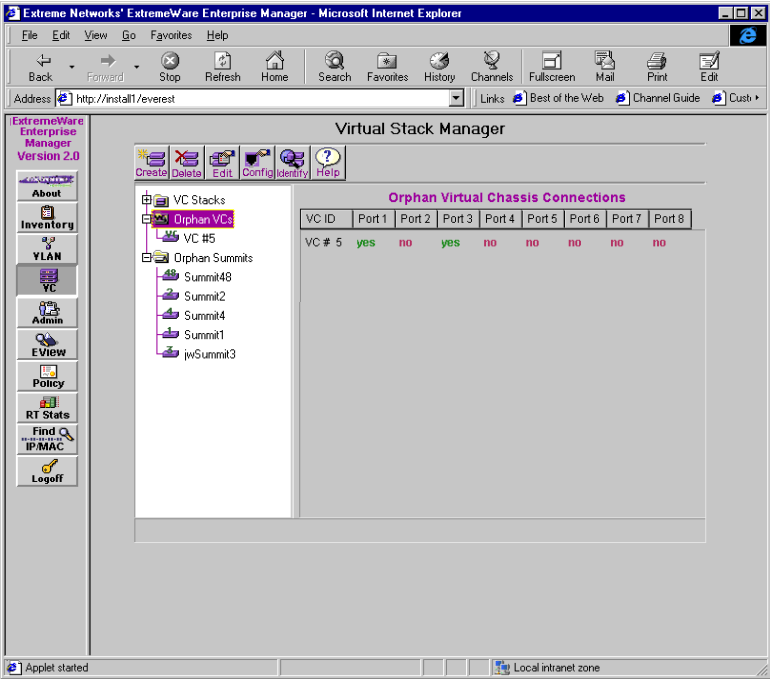


Figure 9-4: Orphan Virtual Chassis Connections

The display shows any ports that have connections to switches, for each Virtual Chassis in the Orphan VC list.

Selecting an individual Virtual Chassis in the Orphan VC list displays a detail diagram similar to that shown in Figure 9-3.

DISPLAYING ORPHAN SUMMIT SWITCHES

The ExtremeWare Enterprise Manager considers a switch to be an orphan if it could not be identified as belonging to a Virtual Chassis stack.

- To display details about the orphan Summit switches, select **Orphan Summits**, as shown in Figure 9-5.

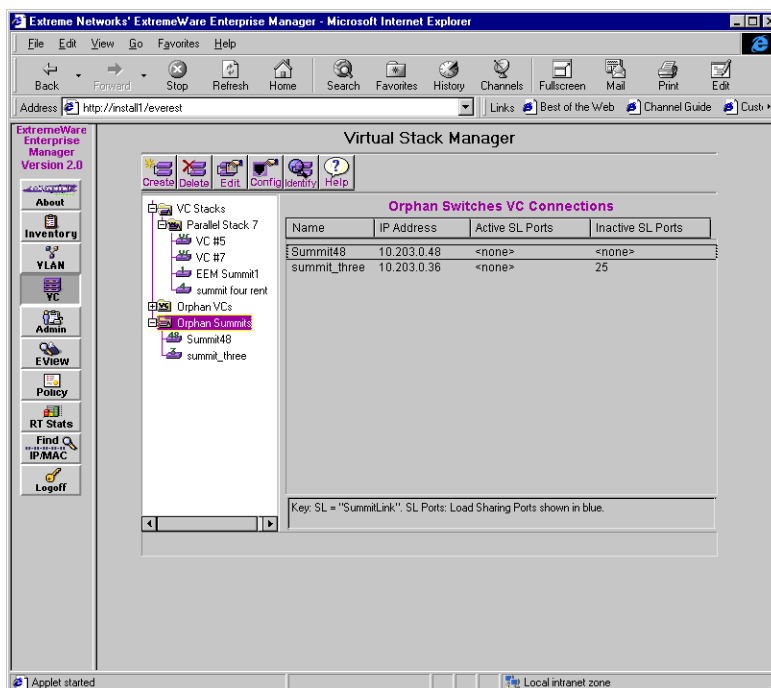


Figure 9-5: Orphan switches Virtual Chassis connections

A Summit may be considered an orphan if:

- It is a member of multiple stacks.
- It has been added to the switch inventory since the last stack identification was done.
- It does not have any VC connections.

The display shows the switch name, the IP address of the switch, and the port numbers of any active and inactive SummitLink ports. If a port is configured as one of a set of load sharing ports, it is displayed in blue. If there are no SummitLink ports, the entries in the Active SL Ports and Inactive SL Ports columns are both **<none>**.

CREATING A VIRTUAL CHASSIS STACK

You must have Administrator or Manager access to create a Virtual Chassis stack.

Creating a Virtual Chassis stack creates a stack representation in the ExtremeWare Enterprise Manager database. It does not change the physical stack configuration or the actual member switch configurations.

To create a new Virtual Chassis stack, click the **Create** button at the top left of the Virtual Chassis Stack Manager window.

The Create VC Stack dialog box appears, as shown in Figure 9-6.

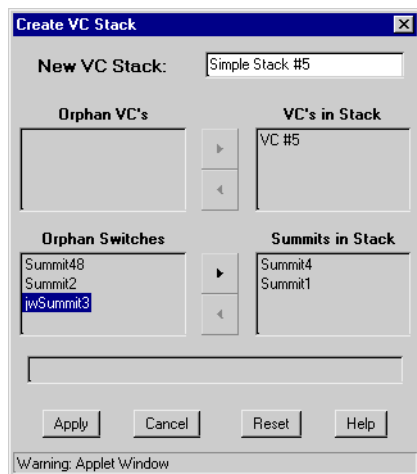


Figure 9-6: Creating a VC stack

To create a Virtual Chassis Stack, follow these steps:

- 1 Type a name for the new stack in the **New VC Stack** field.
- 2 Select one or more Virtual Chassis in the **Orphan VCs** list. Click the right arrow button located between the **Orphan VCs** and the **VCs in Stack** lists. The selected VC is moved to the **VCs in Stack** list.
- 3 To add a Summit switch to the stack, select the switch in the **Orphan Summits** list. Click the right arrow button located between the **Orphan Summits** and the **Summits in Stack** lists. The selected Summit switch is moved to the **Summits in Stack** list.

- 4 To remove a Virtual Chassis from the VC stack, select the Virtual Chassis and click the left arrow button. The selected switch is moved to the **Orphan VCs** list.
- 5 To remove a Summit switch from the VC stack, select the switch and click the left arrow button. The selected switch is moved to the **Orphan Summits** list.
- 6 When you have finished adding and removing switches, click the **Apply** button to add the new Virtual Chassis stack to the ExtremeWare Enterprise Manager database.

Once you have created a Virtual Chassis stack, you may configure the switches in the stack to indicate which ports are in SummitLink mode, and whether they are configured for Load Sharing. See “Configuring Virtual Chassis Stack Ports” for directions on how to do this.

DELETING A VIRTUAL CHASSIS STACK

You must have Administrator or Manager access to delete a Virtual Chassis stack.

Note: *Deleting a Virtual Chassis stack removes the stack representation in the ExtremeWare Enterprise Manager database. It does not affect the actual configuration of the Virtual Chassis or the member switches. The component devices remain in the Enterprise Manager database.*

To delete the representation of a Virtual Chassis stack, click the **Delete** button at the top of the main Virtual Chassis Stack Manager window.

The Delete VC Stack dialog box appears, as shown in Figure 9-7.

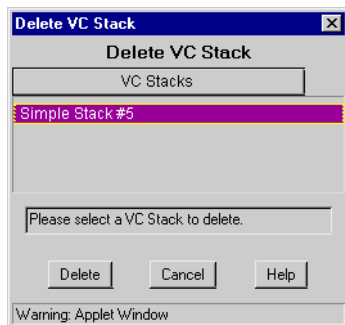


Figure 9-7: Delete Virtual Chassis Stack

To delete a Virtual Chassis stack, select the stack from the **VC Stacks** list, and click the **Delete** button.

If you confirm that you want the stack deleted, the representation of this stack is deleted in the ExtremeWare Enterprise Manager database. It has no effect on the actual devices in your network.

The Virtual Chassis and switches in the Virtual Chassis stack become Orphans, and now appear in their respective Orphan lists.

EDITING A VIRTUAL CHASSIS STACK

You must have Administrator or Manager access to edit a Virtual Chassis stack.

Note: *Editing a Virtual Chassis stack updates the stack representation in the ExtremeWare Enterprise Manager database. It does not affect the actual configuration of the Virtual Chassis or the member switches.*

To edit the ExtremeWare Enterprise Manager's representation of a virtual chassis stack, click the **Edit** button at the top of the main Virtual Chassis Stack Manager window.

The Edit VC Stack dialog box appears, as shown in Figure 9-8.

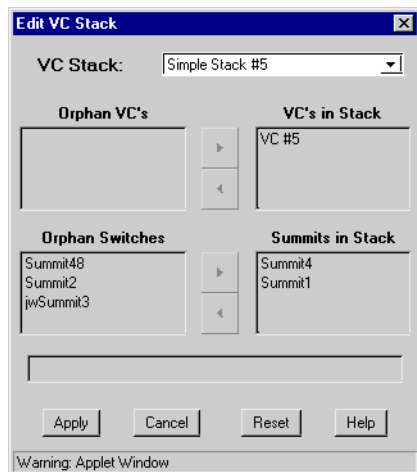


Figure 9-8: Editing a VC stack

To edit a Virtual Chassis Stack, follow these steps:

- 1 Select a Virtual Chassis Stack from the pull down list in the **VC Stack** field.

The dialog box displays all the Summit Virtual Chassis and Summit Switches that are either included in the selected stack, or are considered orphans (not included in any VC stack).

- 2 To add a Summit Virtual Chassis to the stack, select the Virtual Chassis in the **Orphan VCs** list. Click the right arrow button located between the **Orphan VCs** and the **VCs in Stack** lists. The selected VC is moved to the **VCs in Stack** list.
- 3 To add a Summit switch to the stack, select the switch in the **Orphan Summits** list. Click the right arrow button located between the **Orphan Summits** and the **Summits in Stack** lists. The selected Summit switch is moved to the **Summits in Stack** list.

Note: *Each Summit switch and Virtual Chassis may appear in only one VC stack within the Enterprise Manager database.*

- 4 To remove a Summit Virtual Chassis from the VC stack, select the Virtual Chassis and click the left arrow button. The selected switch is moved to the **Orphan VCs** list.
- 5 To remove a Summit switch from the VC stack, select the switch and click the left arrow button. The selected switch is moved to the **Orphan Summits** list.

Note: *There must be at least one Virtual Chassis and one Summit switch in a VC stack.*

- 6 When you have finished adding and removing switches, click the **Apply** button to register the changes in the ExtremeWare Enterprise Manager database.

At any time before you click **Apply**, you can click **Reset** to undo the changes you have made. This restores the Virtual Chassis stack to the state it was in when you started.

When you add a Summit switch to a Virtual Chassis stack, you may also need to configure the switch ports to indicate which ports are in SummitLink mode, and whether they are configured for Load Sharing. See “Configuring Virtual Chassis Stack Ports” for directions on how to do this.

CONFIGURING VIRTUAL CHASSIS STACK PORTS

If you have Administrator or Manager access, you can configure the mode and load sharing attributes of the ports on the Summit switches in a VC stack.

You can also configure the ports on switches in the Orphan Summit list. This is done in the same way as for switches in a VC stack. You may need to do this prior to adding an Orphan switch to a Virtual Chassis stack.

To configure ports, follow these steps:

- 1 Select a VC stack or Orphan Summits in the Component Tree.
- 2 Click **Config** at the top of the Virtual Chassis Stack Manager page.

The Configure Ports in VC Stack dialog Box appears, as shown in Figure 9-9.

Configure Ports for Summits on a VC Stack

Configure Ports in VC Stack: Parallel Stack 7

Switch Name	IP Address	(Gig) Port #	SummitLink Mode	Load Sharing
EEM Summit1	10.203.253.31	1	<input type="checkbox"/>	None
EEM Summit1	10.203.253.31	2	<input type="checkbox"/>	None
EEM Summit1	10.203.253.31	3	<input type="checkbox"/>	None
EEM Summit1	10.203.253.31	4	<input checked="" type="checkbox"/>	2 port
EEM Summit1	10.203.253.31	5	<input checked="" type="checkbox"/>	2 port
EEM Summit1	10.203.253.31	6	<input checked="" type="checkbox"/>	2 port
EEM Summit1	10.203.253.31	7	<input checked="" type="checkbox"/>	2 port
EEM Summit1	10.203.253.31	8	<input type="checkbox"/>	None
summit four rent	10.203.254.34	17	<input checked="" type="checkbox"/>	2 port
summit four rent	10.203.254.34	18	<input checked="" type="checkbox"/>	2 port
summit four rent	10.203.254.34	19	<input checked="" type="checkbox"/>	2 port
summit four rent	10.203.254.34	20	<input checked="" type="checkbox"/>	2 port
summit four rent	10.203.254.34	21	<input checked="" type="checkbox"/>	None
summit four rent	10.203.254.34	22	<input checked="" type="checkbox"/>	None

Apply Cancel Reset Help

Warning: Applet Window

Figure 9-9: Configure ports in a VC Stack

- 3 Select a VC stack, or Orphan Switches, from the pull down list in the field at the top of the dialog box.

Every Gigabit Ethernet port on every switch in the VC stack or the Orphan Summits list is displayed, identified by Switch Name, IP Address, and Port Number.

- The SummitLink Mode box indicates whether the port is configured for connection to a Virtual Chassis. A check indicates the port is in SummitLink mode. No check indicates the port is in Ethernet mode.
- The Load Sharing field indicates whether the port is configured for load sharing. **None** indicates the port is not configured for load sharing. **2 port** or **4 port** indicates the port is configured as one of the ports used for load sharing.

- 4 To change the SummitLink mode for a port, click in the box to turn the check mark on or off. A check mark indicates that the port is in SummitLink mode.

When you change the SummitLink mode for a port that is configured for Load Sharing, Enterprise Manager automatically sets the SummitLink mode configuration for the other port(s) involved in the load sharing.

- 5 To change the Load Sharing configuration, pull down the menu associated with the Load Sharing field for the port, and then select the appropriate value (None, 2 port, or 4 port).

The pull-down menu only presents choices that are valid for the switch type. For example, if the Switch is a Summit1 or a Summit4, you have all three choices (None, 2 or 4 port configuration). For a Summit2 switch, you only have the choice of None or 2 port.

When you select Load Sharing for a port, ExtremeWare Enterprise Manager will automatically set the load sharing configuration for the other port(s) involved in the load sharing. For example, on a Summit2 switch, if you set Port 17 to 2 port, Enterprise Manager also sets Port 18 to 2 port.

See the *Summit Switch Installation and User Guide* for details on load sharing configurations.

IDENTIFYING THE VIRTUAL CHASSIS STACK TOPOLOGY

You must have Administrator or Manager access to force a re-identification of the Virtual Chassis stack topology.

To identify all Virtual Chassis stacks, click **Identify** at the top of the Virtual Chassis Stack Manager page.

The Identify All VC Stacks pop-up dialog appears, as shown in Figure 9-10.

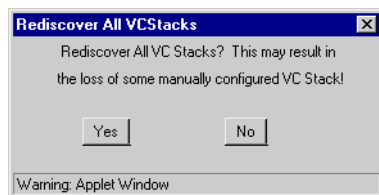


Figure 9-10: Identify Virtual Stack

To use a SNMP identification process to identify Virtual Chassis Stacks, click **Yes**.

ExtremeWare Enterprise Manager runs the SNMP identification process, and redisplay the Component Tree to show the Virtual Stack configuration topology as identified during the discovery process.

Note: *Rediscovering the Virtual Chassis stack causes any manual changes you have made to your Virtual Chassis stack configurations to be lost.*

10

Real Time Statistics

This chapter describes how to use the Real Time Statistics applet for:

- Viewing percentage utilization or total errors data for multiple ports in an Extreme Networks switch, a switch slot, or a port group.
- Viewing historical utilization, total errors, or individual errors data for a specific port on an Extreme Networks switch.

OVERVIEW

The Real Time Statistics feature of ExtremeWare Enterprise Manager enables you to view a graphical presentation of utilization and error statistics for Extreme switches in real time. The data is taken from Management Information Base (MIB) objects in the etherHistory table of the Remote Monitoring (RMON) MIB.

Note: *You must have RMON enabled on the switch in order to collect real-time statistics for the switch.*

This feature is supported only for Extreme Networks switches.

You can view data for multiple ports on a device, device slot, or within a port group, and optionally limit the display to the “top N” ports (where N is a number you can configure). If you choose to view multiple ports, the display shows data for the most recent sampling interval for the selected set of ports. The display is updated every sampling interval.

You can also view historical statistics for a single port. If you choose to view a single port, the display shows the value of the selected variable(s) over time, based on the number of datapoints the MIB maintains in the etherHistory table.

You can choose from a variety of styles of charts and graphs as well as a tabular display.

You can view the following types of data:

- **Percent Utilization** for each port in the set (device, port group, or single port).
Percent utilization reports the value of the **etherHistoryUtilization** MIB object. The MIB defines this variable as follows:

Table 10-1: Definition of RMON utilization variable used in port utilization displays

etherHistoryUtilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in graphed in percents.
--------------------------------	---

- **Total Errors** for each port in the set (device, port group, or single port).
Total Errors is the sum of the six error variables shown in Table 10-2.
- **Individual Errors** for a single port.
An individual errors display shows the six variables shown in Table 10-2.

Table 10-2: Definition of RMON etherHistory error variables for port error displays

etherHistoryCRCAlignErrors	The number of packets received during this sampling interval that had a length between 64 and 1518 octets, inclusive, (excluding framing bits but including Frame Check Sequence (FCS) octets) but that had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherHistoryUndersizePkts	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.

Table 10-2: Definition of RMON etherHistory error variables for port error displays

etherHistoryOversizePkts	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
etherHistoryFragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherHistoryJabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherHistoryCollisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

DISPLAYING MULTIPOINT STATISTICS

When you click the **RT Stats** button in the Navigation Toolbar, the main Real Time Statistics page is displayed as shown in Figure 10-1. Initially, no data is displayed—you see a message asking you to select a device, device slot, or port group to be displayed.

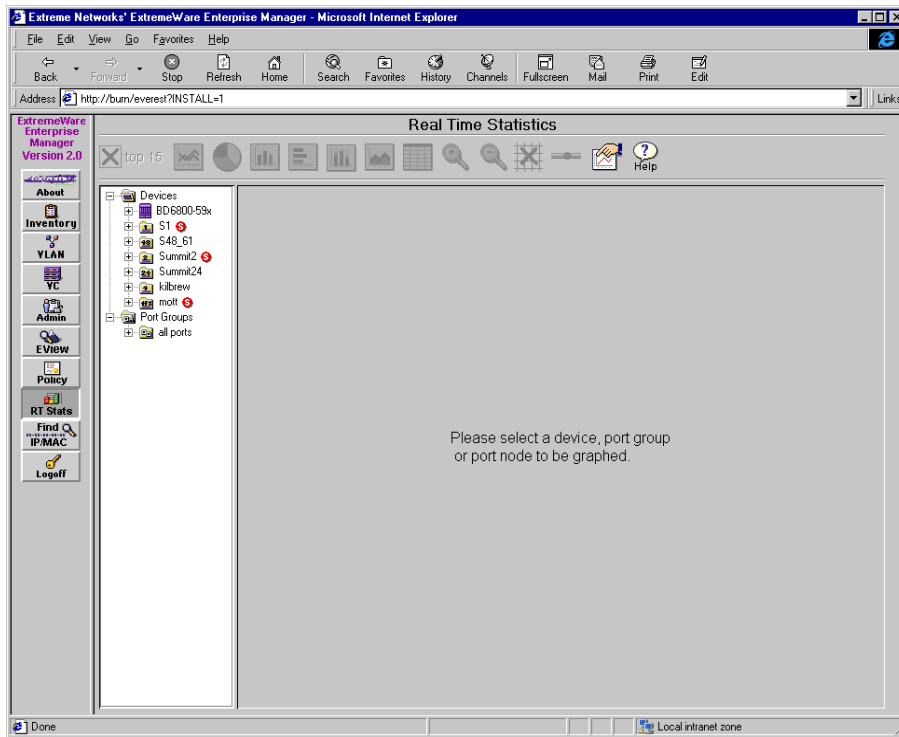


Figure 10-1: Real Time Statistics main page

A device with a red circle “S” next to it indicates that the device is not responding to SNMP requests. A port group with a red circle “S” indicates that the port group is empty.

For an individual port, you can display individual errors in addition to utilization and total errors.

- ◆ Select a network device to display data for some or all ports on the device.
- ◆ Select a port group to display data for all ports in the port group.

You will first see a message saying “Please wait, loading data.” If the ExtremeWare Enterprise Manager is successful, utilization data is displayed, as shown in Figure 10-2.

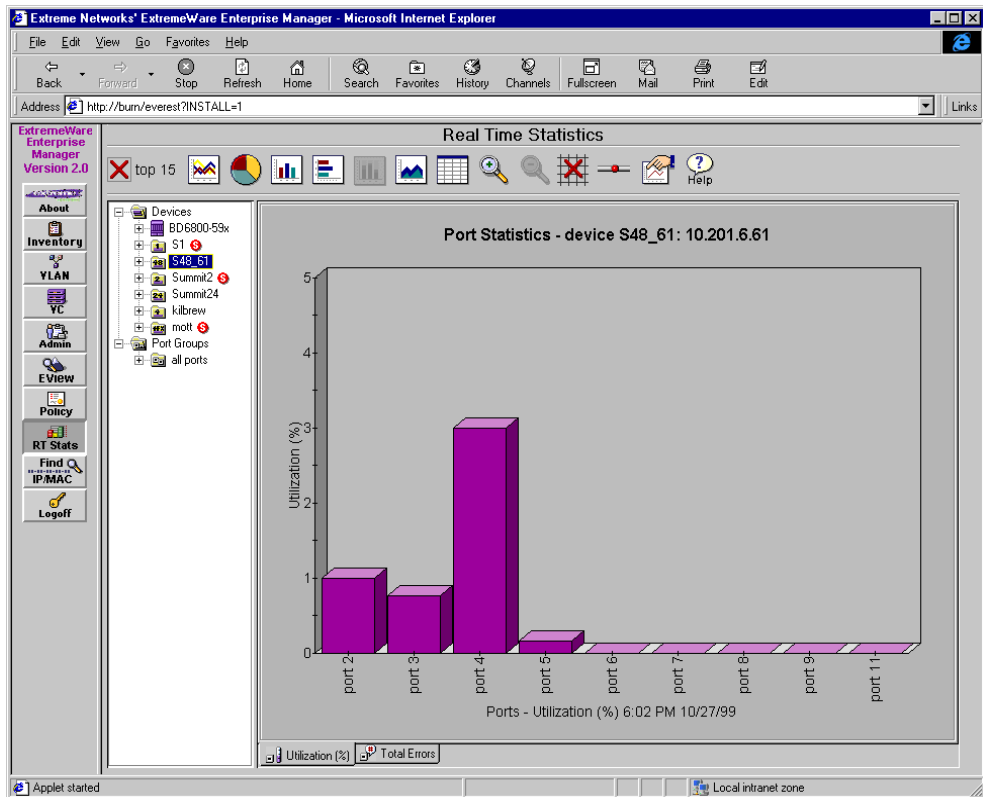


Figure 10-2: Bar chart showing device port statistics

If you place the cursor near a bar in the chart, a pop-up window shows the port number and device, actual data value, and the time stamp on the data sample.

You can use the mouse to change the depth and rotation of a 3-dimensional chart:

- Hold down the [Shift] key, press the left mouse button, and drag the cursor left or right to rotate the graph.
- Hold down the [Ctrl] key, press the left mouse button, and drag the cursor up or down to set the depth of the 3-dimensional view.

For any of the bar graphs, move the cursor and then wait to see the change take effect, which may take a few seconds.

There are cases where you may not see data for every port you expect in a multi-port display:

- You have selected the “top N” feature (top 15 by default), so only the “N” ports with the highest utilization or the highest total number of errors are displayed.
- RMON is disabled for some ports on the switch. If the switch as a whole can be reached and is reporting data, then individual ports that do not report data will be ignored. No error message is presented in this case.

If the Enterprise Manager is *not* successful in loading data from the device, it displays a message similar to that shown in Figure 10-3.

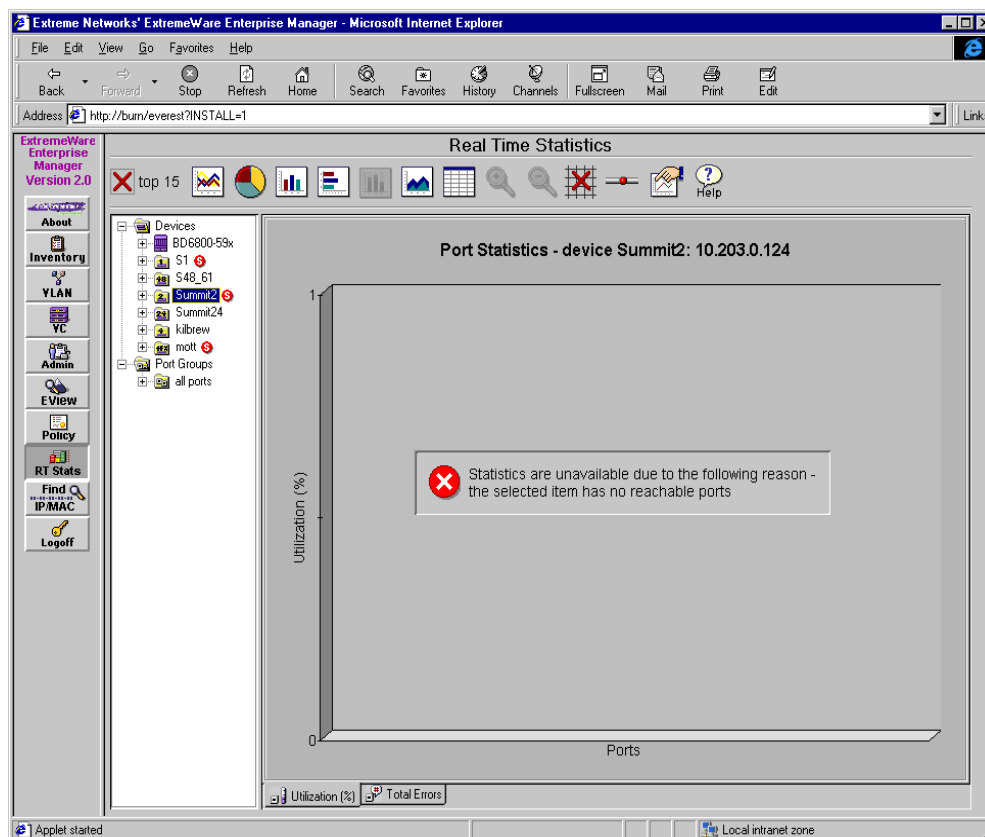


Figure 10-3: Warning displayed when Enterprise Manager cannot retrieve data

There are several reasons why the Enterprise Manager may not be able to display *any* device data:

- The Enterprise Manager cannot communicate with the device (indicated by an “S” in a red circle next to the device name).
- The device does not have RMON enabled, or RMON was just recently enabled and no data samples exist yet.

DISPLAYING STATISTICS FOR A SINGLE PORT

In addition to displaying data for a set of ports, you can display historical data for an individual port. You can select a port in one of two ways:

- Double-click on the data point for an individual port in the device or port group statistics display (bar, data point, or pie slice in the respective chart, or row in a tabular display).
- Click on a device, device slot, or port group in the left-side Component Tree to list the ports it contains, then select a port.

A set of utilization statistics for the selected port is displayed, as shown in Figure 10-4.

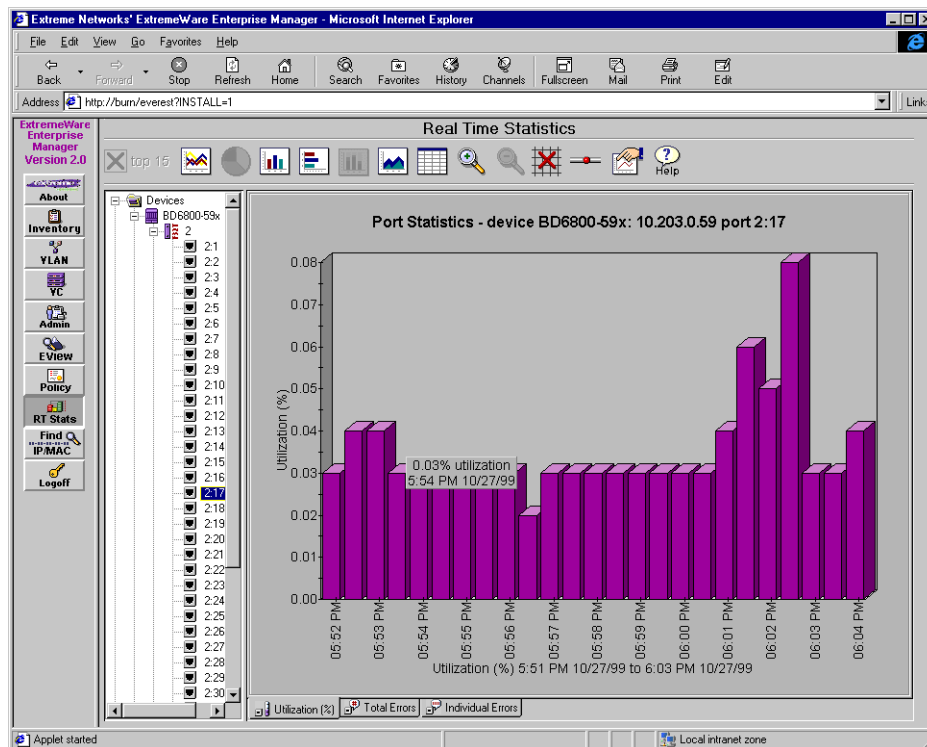


Figure 10-4: Utilization data over time for an individual port on a device.

The number of data points displayed, and the sampling interval are user-configurable parameters, within the limitations of the device configuration. The defaults are:

- A 30-second sampling interval
- 50 data points displayed

However, in Figure 10-4, only 25 data points are displayed, because that is the maximum number of values the BlackDiamond switch stores as historical data.

For an individual port, you can display individual errors in addition to utilization and total errors.

- ◆ Select the tab at the bottom of the page to generate one of these displays. Figure 10-5 is an example.

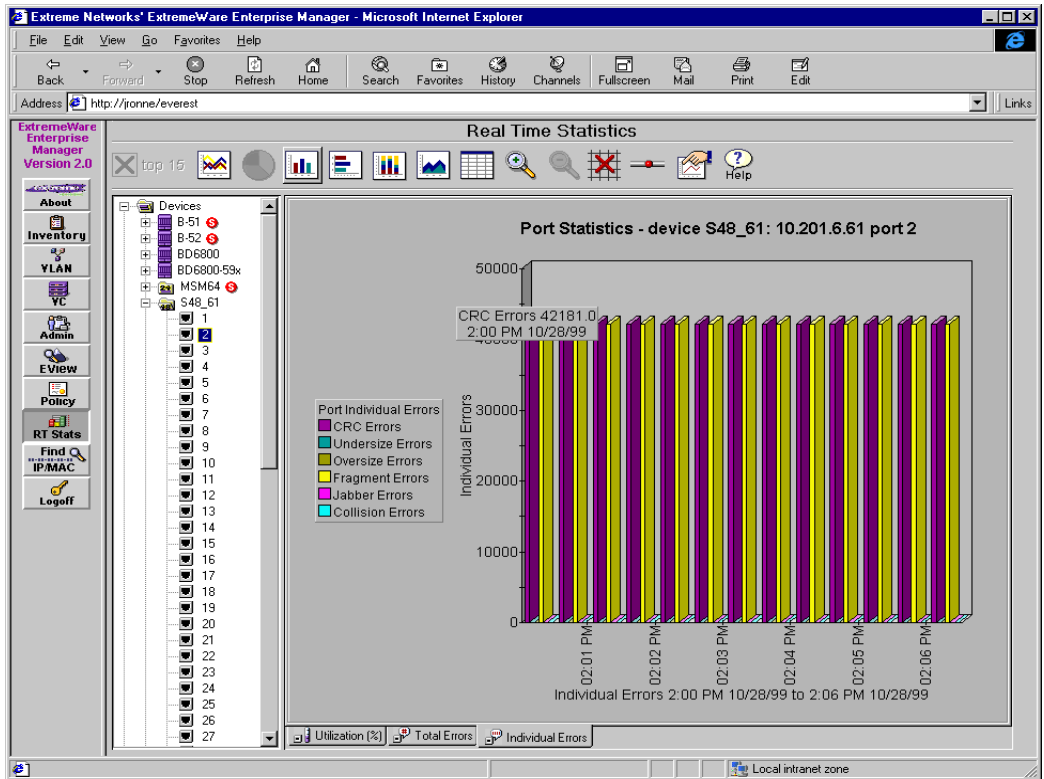


Figure 10-5: Individual errors in a single-port chart

CHANGING THE DISPLAY MODE

The icons at the top of the page let you select the format of the statistical display, and control several other aspects of the display.



top 15



top 15

Select this to determine whether the display for a device or port group will include all ports, or only the top N ports (where N is initially fifteen). Click the icon to toggle between the red X, which indicates the top N limitation is not in effect, and a green check, which indicates that the top N ports are being displayed. The top N ports are displayed in order from highest (largest percent utilization or largest total errors) to lowest. The number of ports (N) is a user-configurable setting. This option is available only for multi-port displays.



Select this to display the data as a line graph. This chart type is especially useful when displaying individual errors for a single port.



Select this to display the data as a pie chart. This chart type is available only when you are displaying statistics for multiple ports on a device, device slot, or in a port group. The maximum number of slices in the pie is a user-configurable setting. It is initially set to display 10 slices.



Select this to display the data as a bar chart. A 3D bar chart is the default for all chart displays. The 3D setting is also a user-configurable option.



Select this to display the data as a horizontal bar chart. This chart type by default displays in 3D. The 3D setting is also a user-configurable option.



Select this to display the data as a stacked bar chart. This chart type is only available when you are displaying individual errors for a single port.



Select this to display the data as an area chart. This chart type by default displays in 3D. The 3D setting is also a user-configurable option.



Select this to display the data as a table.



Select this to zoom in on (magnify) the size of the display. You can select this repeatedly to zoom up to three times the screen size.



Select this to zoom out (shrink) the size of the display. You can select this repeatedly until the chart is the desired size.



Determines whether grid lines are displayed on the background of the chart. Click the icon to toggle between the red X, which indicates that grid lines are turned off, and the green check, which indicates that grid lines are turned on.



Determines whether the graph data is updated automatically at every sampling interval. Click on the icon to toggle between continuous updates, indicated by the bar with the red dot (representing a traveling data packet), and the open palm, indicating that updates have been suspended.



Select this to bring up the graph preferences pop-up window. You can change a variety of settings, such as graph and data colors, the sampling interval, or the number of ports in a top N display.

SETTING GRAPH PREFERENCES

To change the graph settings used in this applet, click the **Set Graph Preferences** icon in the toolbar.

The Graph Preferences window is displayed, as shown in Figure 10-6.

Use the tabs across the top of the window to select the type of setting you want to change. Each tab displays a page with a group of related settings. When you have changed any setting you want on a given page:

- Click **Apply** to put the changes into effect, but stay in the Graph Preferences window so you can make changes on another page.
- Click **OK** to put the changes into effect and close the Graph Preferences window.

Note: *The Graph preferences settings are not persistent—if you move to another ExtremeWare Enterprise Manager applet, the settings will return to the defaults.*

Graph View (Figure 10-6) lets you change from 3D to 2D displays, and change the values for the 3D depth, elevation and rotation.

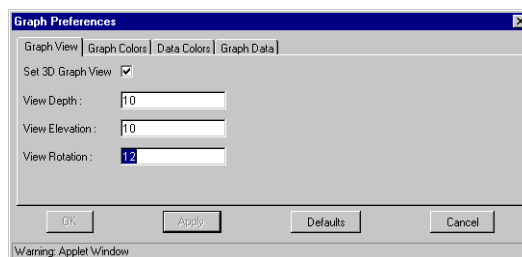


Figure 10-6: Setting 3D graph preferences

- To change to a 2D graph view, click the **Set 3D Graph View** box to remove the check mark.
- **View Depth** controls the depth of a bar. The default is 10, maximum is 1000.
- **View Elevation** controls the elevation (rise) from the front of the bar to the back, in degrees. The default is 10°, range is $\pm 45^\circ$.
- **View Rotation** controls the angle of rotation of the bar, in degrees. The default is 12°, range is $\pm 45^\circ$.

Graph Colors (Figure 10-7) lets you set the colors for the graph background and text (data and axis labels).

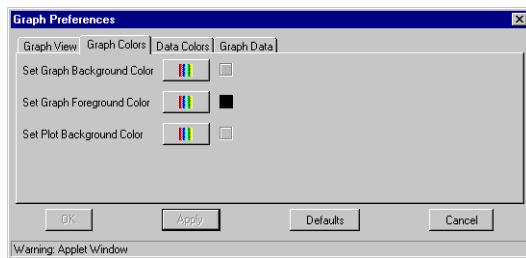


Figure 10-7: Setting graph color preferences

- To change a color, click on a button with the color bar icon. This displays a color selection window where you can select the color you want. You can select a color using color swatches, or by specifying HSB or RGB values.
- **Set Graph Background Color** sets the color of the background surrounding the graph.
- **Set Graph Foreground Color** sets the color of the text and bar outlines.
- **Set Plot Background Color** sets the color of the background behind the graph data.

Data Colors (Figure 10-8) lets you set the colors used for the various data sets in your graph.

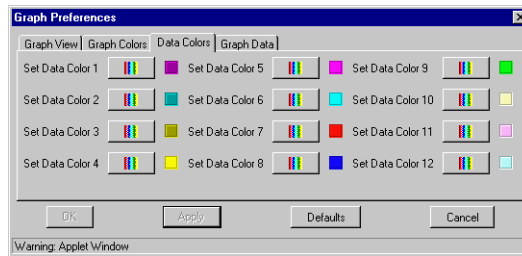


Figure 10-8: Setting data color preferences

- To change a color, click on a button with the color bar icon. This displays a color selection window where you can select the color you want. You can select a color using color swatches, or by specifying HSB or RGB values.
- **Data Color 1** is the color used for Utilization and Total Error graphs.
- Data colors 1 through 6 are used for the different errors in a individual errors chart.
- Data colors in order starting from 1 are used in a pie chart, for as many slices as you've specified. (If you specify more than 12 slices, the colors will repeat, with slice 13 using the same color as slice 1).

Graph Data (Figure 10-9) lets you set several miscellaneous graph parameters.

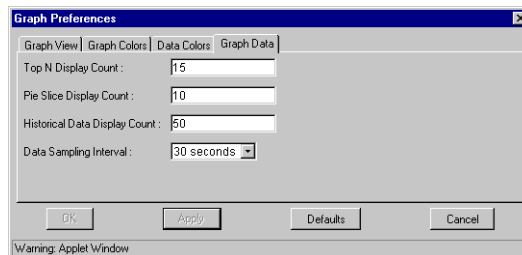


Figure 10-9: Setting other graph preferences

- **Top N Display Count** specifies the number of ports to include in a Top N display. The default is 15, maximum is 100.
- **Pie Slice Display Count** specifies the number of slices to display in a pie chart. The default is 10, maximum is 50.

- **Historical Data Display Count** specifies the number of historical data points to display in a graph for an individual port. The default is 50, the maximum value you can set is 100. However, the actual maximum number of data points you can get is determined by the SNMP agent running in the device from which you are getting data.
- **Historical Data Sampling Interval** is the sampling interval to use when displaying historical data. Select a choice from the pull-down list. The choices in the list are determined by the configuration of the device from which you are getting data.

11

Using the IP/MAC Address Finder

This chapter describes how to use the IP/MAC Address Finder applet for:

- Creating search requests for locating MAC or IP addresses on the network.

OVERVIEW OF THE IP/MAC FINDER APPLET

The IP/MAC Address Finder applet lets you search for network addresses (MAC or IP addresses) and identify the switch and port on which the address resides. The Search Tool lets you configure and start a search task, view the status of the task, and view the task results. The task specification and results are kept in the task list until you delete them, or until you log out of ExtremeWare Enterprise Manager client.

When you click the **Find MAC** button in the Navigation Toolbar, the main IP/MAC Address Finder page is displayed as shown in Figure 11-1. Initially there are no search requests displayed.

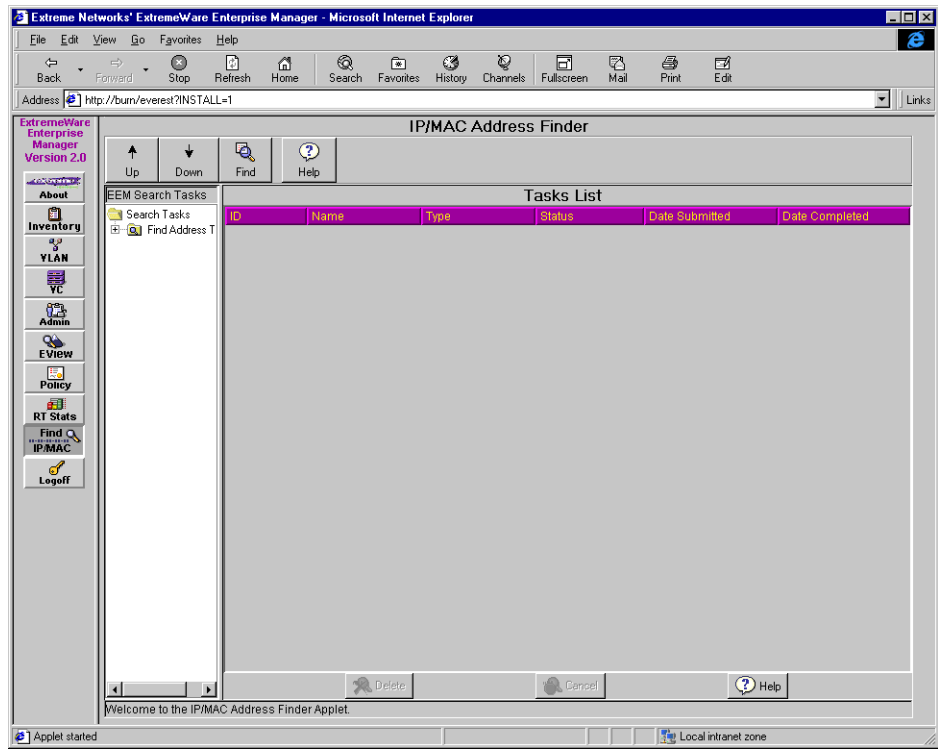


Figure 11-1: IP/MAC Address Finder main page

TASKS LIST SUMMARY WINDOW

As search tasks are initiated, they are placed in the Find Address Tasks List in the Component Tree. Selecting the Find Address Tasks folder in the Component Tree displays a summary of the status of the tasks in the Task List (see Figure 11-2).

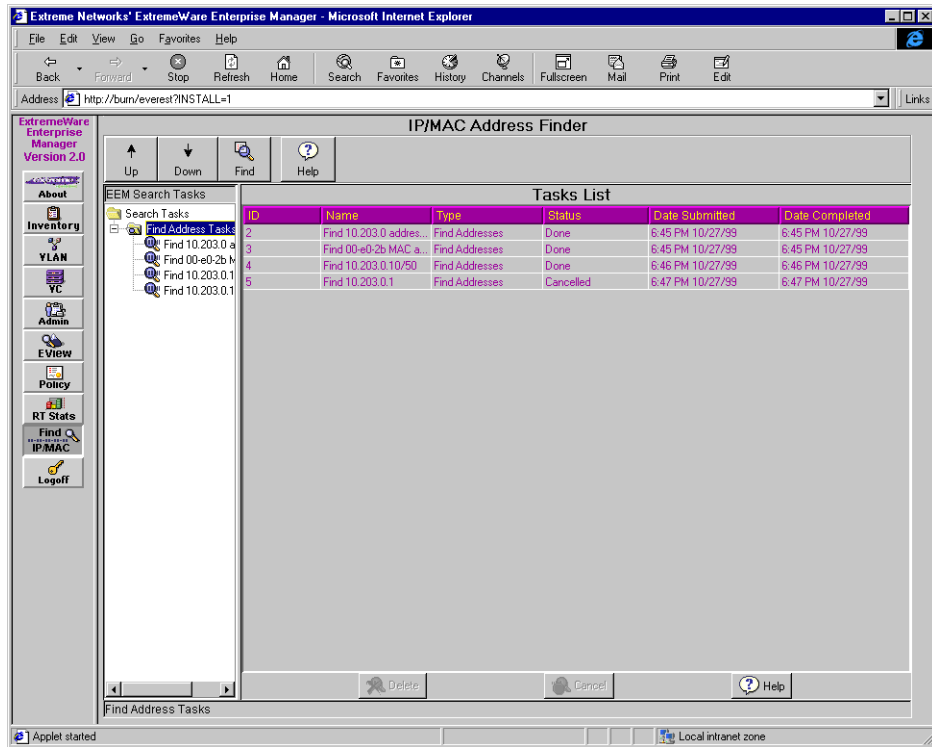


Figure 11-2: Tasks List summary

The Tasks List shows you basic information about the tasks you set up.


- **ID** is automatically assigned by ExtremeWare Enterprise Manager.
- **Name** is the name you gave the task when you created it. Giving a task a unique name is important to distinguish it from other tasks in the Tasks List.
- **Type** is the type of search this will perform. In ExtremeWare Enterprise Manager release 2.0, this is always **Find Addresses**, the only task type available in this release.
- **Status** shows the status of the request. Possible values are Pending, and Done.
- **Date Submitted** shows the date and time the task was submitted.
- **Date Completed** shows the data and time the task was finished.

From the **Tasks List** you can perform the following functions:

- Select a task and click **Delete** to delete an individual task. This deletes the task specification as well as the task results. Once a task has completed, it cannot be rerun unless it is the most recent task completed.
- Select a Pending task and click **Cancel** to cancel the task before it has completed.

Note: *The specified tasks and their search results persist as long as you are running the ExtremeWare Enterprise Manager client, even if you leave the IP/MAC Address Finder applet and go to another Enterprise Manager applet. However, when you exit the Enterprise Manager client, all the task specifications and search results are deleted.*

CREATING A SEARCH TASK

To create a search task, click the Search Task button  in the tool bar at the top of the IP/MAC Address Finder page. This displays the Find Addresses window (Figure 11-3).

Note: *If you have already submitted a task, the most recent task with its specifications is displayed in the Find Addresses window.*

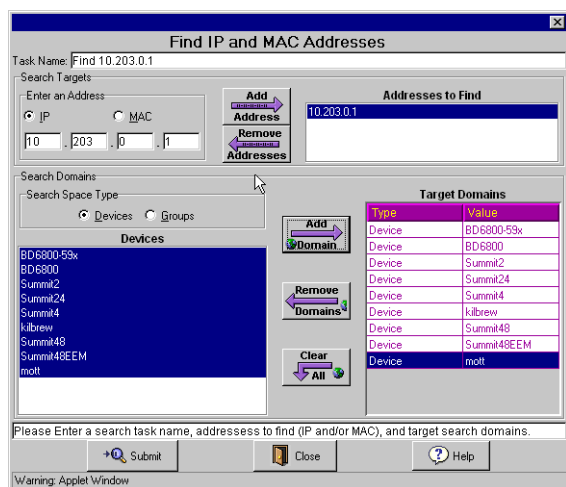


Figure 11-3: Find addresses window

To create a search task:

- 1 Enter the task name in the **Task Name** field. This name helps you identify the task in the Find Address Tasks List.
- 2 Define the search targets: select either **IP** or **MAC** to determine the format of the address to search for, and enter the address into the fields provided. Click the **Add Address** button to add the address to **Addresses to Find** list.

Click the **Remove Address** button to remove an address from the list.

- 3 Define the search domain. **Target Domains** specifies the scope of the devices to be included in the search. Devices not included in this domain will not be searched.

You can define the search space in several ways:

- **Devices** lets you select individual devices to include in the search.
- **Groups** lets you search all the devices in a specified Device Group.

You can create a target domain that includes a combination of these specifications.

When you select a Search Space Type, you are presented with a list of the Devices, or Device Groups from which you can select individual members to include in the Target Domains.

- 4 Select the Device or Device Group you want to search and click **Add Domain** to move it into the Target Domains list.
To remove a member of the Target Domains list, select the item in the list and click **Remove Domain**. To clear the Target Domains list, click **Clear All**.
- 5 When you have the search specification defined, click the **Submit** button at the bottom of the window to initiate the search.

DETAILED TASK VIEW

When you initiate a search, the task is placed in the Find Address Tasks list in the Component Tree. The main panel displays the Detailed Task View for the current search task (see Figure 11-4).

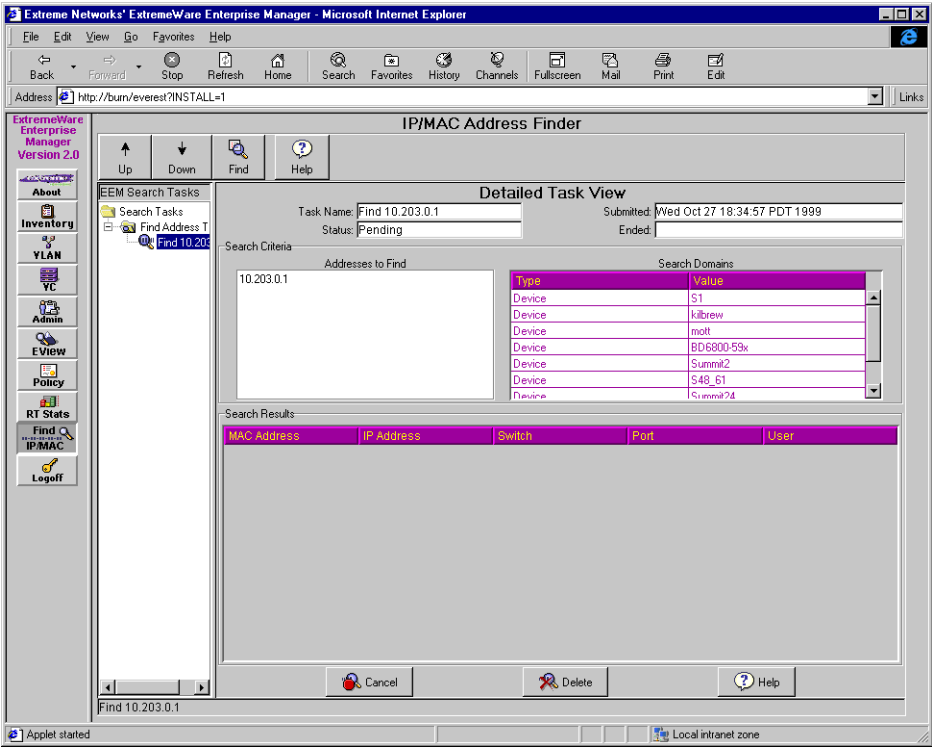


Figure 11-4: Search in progress

While the task is in progress, the window shows the status as **Pending**. When the search is complete, the **Detailed Task View** shows the results for the search (Figure 11-5).

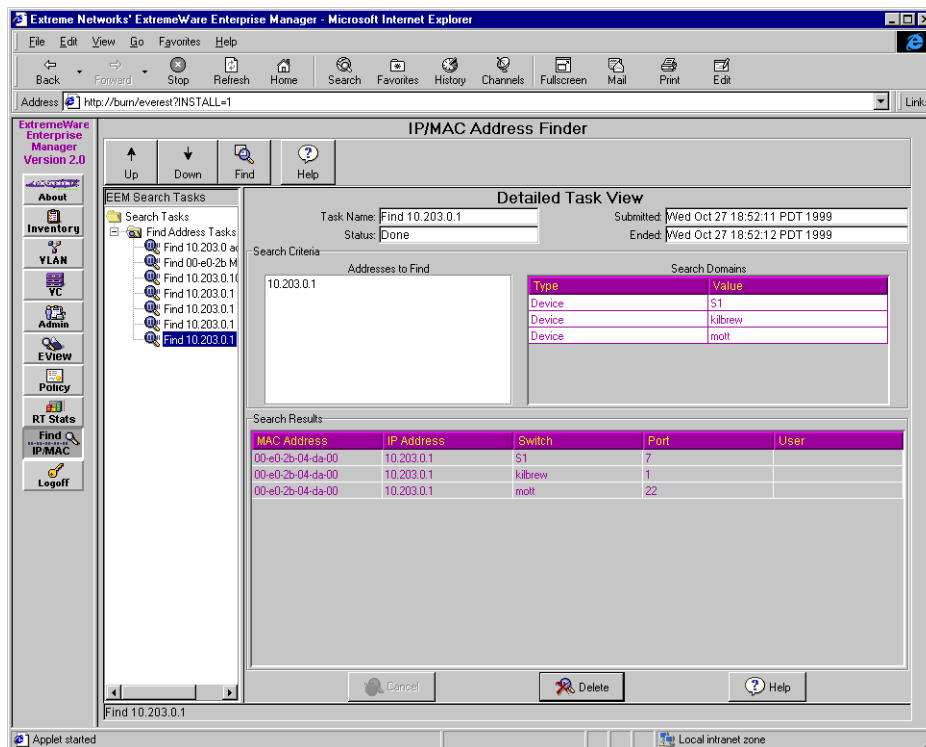


Figure 11-5: Address search results in the Detailed Task View

The Detailed Task View shows the following information about your search.

- **Name** is the name you gave the task when you created it. Giving a task a unique name is important to distinguish it from other tasks in the Tasks List.
- **Status** shows the status of the request. Possible values are Pending, and Done.
- **Date Submitted** shows the date and time the task was submitted.
- **Date Completed** shows the data and time the task was finished.

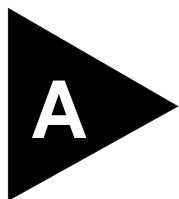
The Search Criteria areas shows:

- The list of IP or MAC addresses that were the object of the search.
- The Search Domains where the search took place. The Search Domains lists shows the name and type (Device or Group) of the components of the domain specification.

The Search Results list shows the results of the search. For every address successfully located, this list shows:

- Both the MAC address and the corresponding IP address.
- The switch and port to which the address is connected
- The User (name) currently logged in at that address.

Once the search is complete, the Search Results will stay in the Tasks List until you explicitly delete them using the Delete Function from the Tasks List Summary View, or until you exit the ExtremeWare Enterprise Manager client.



HP OpenView Integration

This appendix describes:

- Integrating the ExtremeWare™ Enterprise Manager and ExtremeWare Vista components for HP OpenView.
- Launching the Enterprise Manager client and ExtremeWare Vista from HP OpenView.

INTEGRATION OVERVIEW

The HP OpenView integration process makes it possible to launch the ExtremeWare Enterprise Manager client from within HP OpenView. The Enterprise Manager can be launched from the HP OpenView Network Node Manager Tools menu, or from an icon on the Network Node Manager toolbar.

To enable this feature, you need to run the ExtremeWare HP OpenView integration process on the server where your HP OpenView platform is running. This also requires that you have a Java-enabled Web browser installed on the system where HP OpenView resides.

The ExtremeWare HP OpenView integration process also provides integration with ExtremeWare Vista.

The HP OpenView software does not need to be running on the same platform type as the ExtremeWare Enterprise Manager. For example, you can install the ExtremeWare Enterprise Manager on a Window NT system, but launch the Enterprise Manager client from an HP OpenView system installed on a SPARC Solaris system.

INTEGRATING WITH HP OPENVIEW UNDER WINDOWS NT

In order to launch ExtremeWare Enterprise Manager and ExtremeWare Vista from HP OpenView under Windows NT, you must add commands to the appropriate HP OpenView menus with links to the Extreme Networks software. In addition, the Extreme Networks MIBs need to be included in the set of MIBs available to HP OpenView. The integration process provided with ExtremeWare Enterprise Manager adds the needed components.

INSTALLING THE HP OPENVIEW INTEGRATION COMPONENTS

If you are installing the ExtremeWare Enterprise Manager on the same server as HP OpenView, you can proceed with the integration as part of the installation script. If this is the case, the Enterprise Manager installation process will bring you to Step 5 below.

To run the integration process, follow these steps:

- 1 Close any open applications.
- 2 Insert the CDROM into the CDROM drive.

If the ExtremeWare Enterprise Manager Welcome screen appears automatically, just exit the install.
- 3 Choose **Run** from the Start Menu.
The Run dialog box appears.
- 4 Type **d:\nt\hpov\setup** in the text box and click **OK**.
If the CDROM is not drive d, substitute the correct drive letter.

The HP OpenView Integration Welcome screen appears.
- 5 Follow the on-screen instructions to progress through the Welcome screen, accept the license agreement, and enter your company information.

The integration process verifies that you have the required version of the HP OpenView software installed. It also checks to see whether you have previously run the ExtremeWare Enterprise Manager integration process.
- 6 In the Installation Type Dialog Box, select which integration to perform:
 - Click **ExtremeWare Vista** to integrate ExtremeWare Vista with the Network Node Manager.
 - Click **ExtremeWare Enterprise Manager** to integrate the Enterprise Manager with the Network Node Manager.

- Click **Extreme Networks supported MIBs** to install Extreme Network's Management Information Base (MIB) definitions. This is necessary for HP Openview to recognize and manage Extreme Networks Summit devices.
- 7 If you are installing the ExtremeWare Enterprise Manager, the **Get ExtremeWare Enterprise Manager Location** Dialog Box is displayed. Type the name of the host where the ExtremeWare Enterprise Manager is installed, and the port number used by the ExtremeWare Enterprise Manager web server.

The port number is the one you specified when installing the ExtremeWare Enterprise Manager web server, by default port 80.

The integration process asks you to verify the configuration you've specified. The integration software now copies the program files to your system.
 - 8 In the next dialog Box, click **Yes** to integrate the MIBs into HP OpenView. This runs the HP OpenView commands to load the MIBs.

If you choose to do this at a later time, you can run the HP OpenView **loadmib.bat** command, found in the HP OpenView `bin` directory.
 - 9 In the next dialog Box, click **Yes** to update the HP OpenView topology database to include the Extreme Networks configuration information. This adds the Summit sysOIDs (system Object IDentifiers) to the HP OpenView topology database, and updates any Summit devices on the map to use Summit-specific icons rather than generic device icons.

This process shuts down the HP OpenView services.

Note: *ExtremeWare Vista is only available when you have selected a Summit device on the Network Node Manager map. You must add the Extreme Networks configuration information to the topology database so the Network Node Manager can recognize Summit devices. Until you do this, you will not be able to access ExtremeWare Vista from Network Node Manager.*

If you choose to do this at a later time, you can run the **OVExtreme.bat** command, found in the HP OpenView `bin` directory.
 - 10 In the final dialog Box, click **Yes** to restart the HP OpenView daemons.

UNINSTALLING THE INTEGRATION COMPONENTS

To uninstall the HP OpenView integration, follow these steps:

- 1 From the Start menu, highlight **Settings**, pull right, and click on the Control Panel. This displays the Control Panel folder.
- 2 Shut down the Enterprise Manager components if they are still running. See “Shutting Down the Enterprise Manager Server Components” in Chapter 3.
- 3 From the Control Panel folder, double-click **Add/Remove Programs**. This displays the Add/Remove Program Properties widow.
- 4 From the list of installed programs select **Extreme Networks HP OpenView 5.01 Integration** and click **Add/Remove**. Follow the instructions to remove the component.

INTEGRATING WITH HP OPENVIEW UNDER SOLARIS

In order to launch ExtremeWare Enterprise Manager and ExtremeWare Vista from HP OpenView under Solaris, you must add commands to the appropriate HP OpenView menus with links to the Extreme Networks software. In addition, the Extreme Networks MIBs need to be included in the set of MIBs available to HP OpenView. The integration process provided with ExtremeWare Enterprise Manager adds the needed components.

INSTALLING THE HP OPENVIEW INTEGRATION COMPONENTS

The following sections assumes that you are running in a command or xterm window.

You must have write access to the HP OpenView directories to perform the Enterprise Manager integration with HP OpenView under Solaris.

To run the integration process, follow these steps:

- 1 Insert the ExtremeWare Enterprise Manager CDROM into the CDROM drive.
- 2 If you are running CDE, the contents of the CDROM are displayed in the File Manager. Go to the **solaris** directory.

To run from an X-term window:

```
cd cdrom/eem2_0/solaris
```

- 3 Run the installation script:

```
./hpovint.sh install
```

- 4** The script begins with an identifying message, and asks you to view and accept the Extreme Networks licensing terms:

```
*****
```

```
Welcome to the Extreme Networks HP OpenView Integration Script
This program will integrate ExtremeWare MIBs
and links into your HP OpenView installation.
```

```
*****
```

```
Extracting temporary files to /tmp/eemovtmp
Please review the following software license terms
and conditions. You will need to accept this license
to continue the installation. Press space to page
through the license.
Press <enter> to view the license:
```

Press [space] or [Enter] to view the license either page-by-page or in one display.

- 5** You are then asked to accept the license terms:

```
The Software and the accompanying documentation are Copyrights of Extreme
Networks
Do you agree to the above conditions? (Y/N): y
```

Enter Y or [Enter] to agree or N to terminate the installation.

- 6** The script next informs you of the steps it will take to install the integration software, and asks you to confirm you want to proceed.

```
This script will copy bitmap and configuration files into your OpenView
installation. It will also add entries to the oid_to_type and oid_to_sym
files. Optionally, xmnloadmib will be used to load the Extreme Networks
mib.
```

```
To update the OpenView database, we will stop OpenView, run ovttopofix, and
optionally restart OpenView.
```

```
Do you wish to continue? (Y/N) [Y]: y
```

Enter Y or [Enter] to continue or N to terminate the installation.

- 7** Next, you are asked for the location of the HP OpenView software.

Please enter the location of your OpenView installation.

Install Directory [/opt/OV]:

Press [Enter] to accept the default, or enter the path and directory where the HP OpenView software is located.

The integration process verifies that you have the required version of the HP OpenView software installed in that location.

8 Enter the appropriate answers to the following questions:

Would you like to integrate ExtremeWare Vista?: (Y/N) [Y]:

Would you like to integrate ExtremeWare Enterprise Manager (EEM)?: (Y/N) [Y]:

Please enter the EEM Server [<eem-server-host>]

The default is the host upon which you are running the installation script.

Please enter the http port used by EEM: [80]

Would you like to update the installed MIBs?: (Y/N) [Y]:

Installation of Extreme Network's Management Information Base (MIB) definitions is necessary for HP OpenView to recognize and manage Extreme Networks devices.

9 The script then asks you to confirm the installation/integration instructions:

*** Configuration

Please review the following items:

```
Vista Integration   = YES
EEM Integration    = YES
EEM Port           = 80
EEM Server         = <eem-server-host>
Update MIBS       = YES
```

Are these correct? (Y to accept / N to re-enter) [N]:y

10 If you answer N, the script asks for these choices again.

Upon a Y or [Enter], the integration software then updates the appropriate HP OpenView files.

Updating OV files...


```

Updating /etc/opt/OV/share/conf/oid_to_type...
(This may take a few moments)
Removing any previous ExtremeNetworks entries in
/etc/opt/OV/share/conf/oid_to_type
Appending new entries to /etc/opt/OV/share/conf/oid_to_type
Done

Updating /etc/opt/OV/share/conf/oid_to_sym...
Removing any previous ExtremeNetworks entries in
/etc/opt/OV/share/conf/oid_to_sym
Appending new entries to /etc/opt/OV/share/conf/oid_to_sym
Done

Copying bitmap files to /etc/opt/OV/share/bitmaps/C/connector
Copying bitmap files to /etc/opt/OV/share/bitmaps/C/toolbar
Copying field files to /etc/opt/OV/share/fields/C
Copying symbol files to /etc/opt/OV/share/symbols/C
Copying registration file summitweb to /etc/opt/OV/share/fields/C
Enabling Vista Selections in /etc/opt/OV/share/registration/C/summitweb
Enabling EEM Selections in /etc/opt/OV/share/registration/C/summitweb
Updating Mibs...
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/rfc1493.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/rfc1757.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/rfc1513.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/rfc2021.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/rfc2239.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/extreme.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/rfc1354.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/rfc1724.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/rfc2037.mib
/opt/OV/bin/xnmloadmib -replace -load data/snmp_mibs/smon.mib

Done

```

The script now shuts down the HP OpenView services, restarts the HP OpenView topology database, and updates the database.

```

/opt/OV/bin/ovstop -v
ovstop: ovspmd is not running
/opt/OV/bin/ovstart ovwdb
/opt/OV/bin/ovw -fields
/etc/opt/OV/share/fields/C/BlackDiamond: Verified Boolean field
"isBlackDiamond"

```

```

/etc/opt/OV/share/fields/C/BlackDiamond: Verified Enumeration field
"SNMPAgent"
  Verified enumeration value "Extreme Networks BlackDiamond" (134)
/etc/opt/OV/share/fields/C/ip_fields: Verified String field "IP Address"
/etc/opt/OV/share/fields/C/ip_fields: Verified String field "IPX Address"
.
.
.

```

When this process has finished, the script runs a process to update the HP OpenView topology database to include the Extreme Networks configuration information. This adds the Summit sysOIDs (system Object IDentifiers) to the HP OpenView topology database, and updates any Summit devices on the map to use Summit-specific icons rather than generic device icons.

```

/opt/OV/bin/ovstart ovtopmd
/opt/OV/bin/ovtopofix -u -o 1.3.6.1.4.1.1916.2.1
Updating S1 (objid = 1584)
/opt/OV/bin/ovtopofix -u -o 1.3.6.1.4.1.1916.2.2
Updating VLAN1 (objid = 1552)
Updating Summit2 (objid = 1678)
Updating Summit2 (objid = 1820)
Updating Summit2 (objid = 4936)

```

11 Finally, you are asked if you want to restart the HP OpenView services. If you answer N you will need to restart them manually before you can use HP OpenView.

```
Would you like to restart the OpenView services now? (Y/N): y
```

```
Restarting OpenView Services
```

```

object manager name: OVSPMD
state:                RUNNING
PID:                  22893
last message:         -
exit status:          -

```

```

object manager name: ovwdb
state:                RUNNING
PID:                  22894
last message:         Initialization complete.
exit status:          -

```

```

.
.
.

```

12 When the process has finished, it returns to the UNIX prompt.

```
script done on Fri 22 Oct 1999 11:23:28 AM PDT
```

Note: *ExtremeWare Vista is only available when you have selected an Extreme device on the Network Node Manager map. You must add the Extreme Networks configuration information to the topology database so the Network Node Manager can recognize Extreme switches. Until you do this, you will not be able to access ExtremeWare Vista from Network Node Manager.*

UNINSTALLING THE INTEGRATION COMPONENTS

A script is provided for uninstalling the HP OpenView integration.

To uninstall the HP Openview integration, do the following:

- 1 Insert the ExtremeWare Enterprise Manager CDROM into the CDROM drive.
- 2 If you are running CDE, the contents of the CDROM are displayed in the File Manager. Go to the `solaris` directory.

To run from an X-term window:

```
cd cdrom/eem2_0/solaris
```

- 3 Run the installation script:

```
./hpovint.sh uninstall
```

LAUNCHING THE CLIENT FROM HP OPENVIEW

If you have run the integration process for HP OpenView, you can launch the ExtremeWare Enterprise Manager client directly from the HP OpenView user interface. You can launch the ExtremeWare Enterprise Manager and ExtremeWare Vista from the Tools menu, or from a pop-up menu associated with a Summit Device icon on the HP OpenView map.

LAUNCHING THE CLIENT FROM THE HP OPENVIEW TOOLS MENU

You can launch either ExtremeWare Enterprise Manager or ExtremeWare Vista from the Network Node Manager's Tool menu, as shown in Figure A-1.

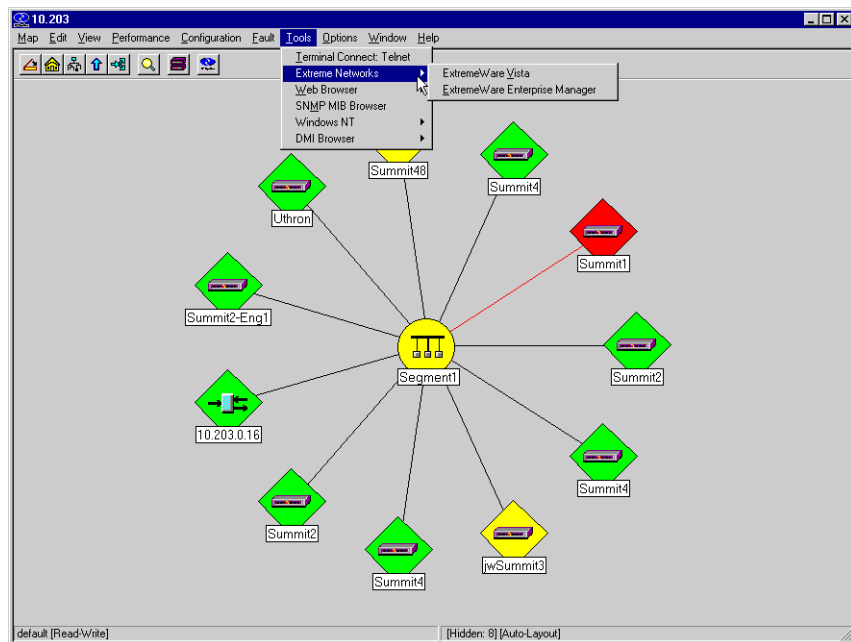


Figure A-1: The Tools menu in HP OpenView Network Node Manager

To launch either ExtremeWare Enterprise Manager or ExtremeWare Vista, follow these steps:

- 1 Click **Tools** to drop down the Tools menu.
- 2 Click **Extreme Networks** to display the ExtremeWare menu.
- 3 Click **ExtremeWare Enterprise Manager** or **ExtremeWare Vista** to launch the appropriate application.

If you have selected a Summit device on the Node Manager Map you will be able to launch ExtremeWare Vista on that device. If you do not have a Summit device selected, the ExtremeWare Vista choice will not be available.

You can also launch ExtremeWare Enterprise Manager from an icon on the Network Node Manager toolbar, as shown in Figure A-2.

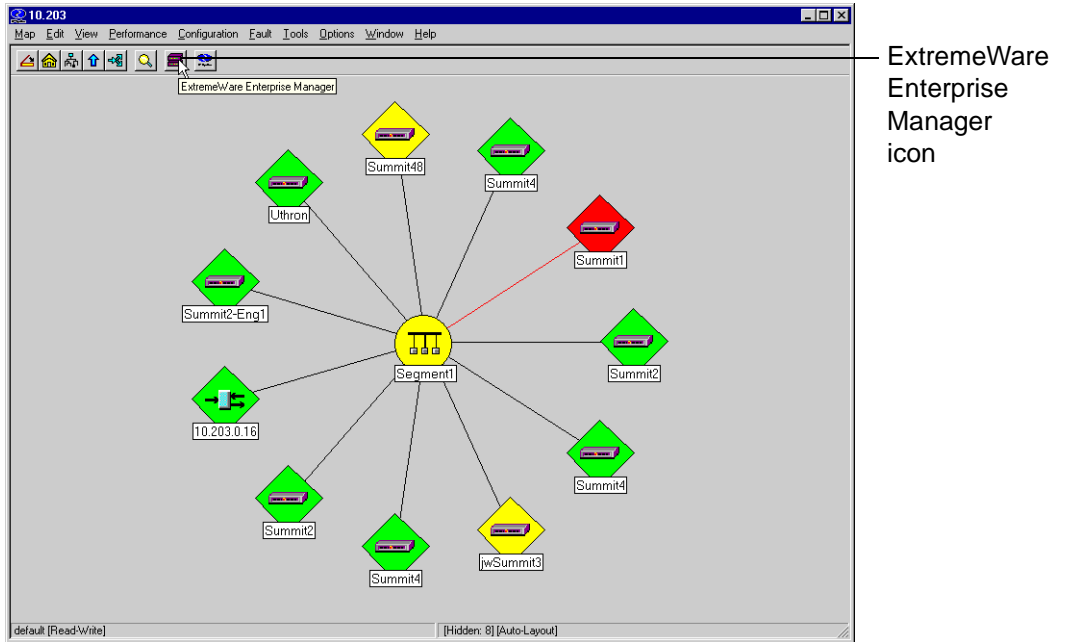


Figure A-2: ExtremeWare Enterprise Manager icon on the HP OpenView toolbar

LAUNCHING EXTREMEWARE VISTA FROM THE HP OPENVIEW MAP

You can launch ExtremeWare Vista for an individual Extreme device directly from the Network Node Manager map using the pop-up menu associated with the device icon.

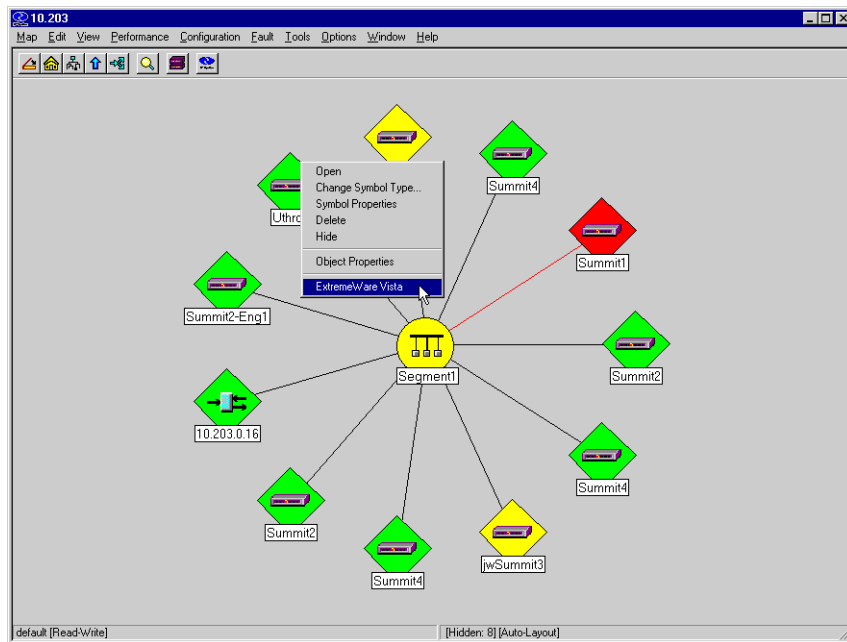


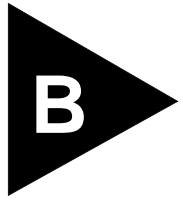
Figure A-3: Pop-up menu for a selected Summit device

To Launch ExtremeWare Vista, follow these steps:

- 1 Select a Summit device on the Network Node Manager Map.
- 2 Click with the right mouse button to display the pop-up menu.
- 3 Click **ExtremeWare Vista** in the menu.

This will launch a browser window and run the ExtremeWare Vista application for the Summit switch you have selected.

For information on using ExtremeWare Vista, see “Using ExtremeWare Vista” in the *Summit Switch Installation and User Guide*.



Dynamic Link Context System (DLCS)

This appendix describes:

- How the ExtremeWare Enterprise Manager policy system uses The Dynamic Link Context System (DLCS) to map logical endstations (users, hosts) to physical attributes.
- How to enable DLCS on Extreme switches running ExtremeWare 5.0 or later.
- Limitations with DLCS as implemented in ExtremeWare 5.0.

OVERVIEW

DLCS is a feature that snoops Windows Internet Naming Service (WINS) NetBIOS packets and creates a mapping between a user name, the IP address of the host (end station) and the switch and port. Based on the information in the packet, DLCS can detect when an end station boots up or shuts down, or a user logs in or logs out. When an end station boots up, DLCS associates its name and IP address to a port on a switch. Similarly, when a user logs in, DLCS associates the user with an end station, and thus a switch port. Such learned information is discarded when the user logs out, or when the end station is shut down.

This information is used by the ExtremeWare Enterprise Manager in setting policies that can be applied to users. These policies can dynamically follow a user's location if auto configuration of policies is enabled. For DLCS to operate within ExtremeWare, the user or end station must allow automatic DLCS updates. This feature should only be used in conjunction with the ExtremeWare Enterprise Manager Policy System.

ExtremeWare Enterprise Manager uses DLCS information to create a policy object for a user or end station that is mapped to the appropriate physical attributes (IP address and switch, port).

USING DLCS IN THE POLICY SYSTEM

For DLCS to operate within the ExtremeWare Enterprise Manager Policy System, two conditions must be met:

- DLCS must be enabled on the switch.
- In the Policy System client, the user or end station must be set to allow automatic DLCS updates.

If both of these conditions are true, then the policy system will expect to get current physical attributes for the user or end station dynamically through DLCS. If auto configuration is enabled in the Policy System client, then dynamic data learned through DLCS will also update the configured policies.

DLCS PROPERTIES

The following guidelines must be used when using DLCS:

- Only one user can be attached to an end station (host) at a given time. This will be the last user that logged in.
- A user may be logged into many end stations simultaneously.
- An IP address can be learned on only one port in the network at a given time.
- Multiple IP addresses can be learned on the same port.
- DLCS mapping is flushed when a user logs in or logs out or when an end station is shut down.

ENABLING DLCS ON AN EXTREME SWITCH

DLCS must be enabled on the switch in order for Enterprise Manager to make use of the capability. It cannot be enabled directly from the Enterprise Manager, it must be enabled using the ExtremeWare CLI through Telnet. Thus, DLCS is not an option under

the ExtremeView Configuration features. However, you can use the ExtremeView Telnet feature to access the switch and enable DLCS.

To enable DLCS on a switch, do the following:

- 1 Click the **ExtremeView** icon in the ExtremeWare Enterprise Manager Navigation Toolbar
- 2 Select **Telnet** in the component tree, then select the switch you want to configure.
- 3 Use the `enable dlcs` command to enable DLCS snooping of packets on the switch.
- 4 Enable the ports on which you want to snoop. You can enable individual ports, or all ports on the switch.

```
enable dlcs ports <port-number>|all
```

DLCS should be enabled on all edge ports (ports that are directly connected to workstations, servers, and unintelligent hubs. DLCS should not be enabled on trunk or uplink ports.
- 5 To see which ports are snooping WINS packets, and what data has been learned:

```
show dlcs
```
- 6 To clear all DLCS data that has been learned:

```
clear dlcs
```
- 7 Type `quit` to exit the telnet session.

DLCS LIMITATIONS

There are certain limitations in the ExtremeWare 5.0 implementation of DLCS that should be considered with regards to the data received from WINS snooping:

- DLCS will not work for the WINS server itself. This is because the WINS server will not send NetBIOS packets on the network (these packets are address to itself). This means that the host name of the WINS server, and any users on the WINS server will not be learned by DLCS.
- When the IP address of an end station is changed, and the end station is not immediately rebooted, the old end station to IP address mapping will never be deleted. You must delete the mapping of the end station to IP address through the ExtremeWare Enterprise Manager Policy System client.
- When an end station is moved from one port to another port on a switch, the old entry will not age out, unless the end station is rebooted or a user login operation is performed after the end station is moved.

- DLCS information is dynamic. Therefore if the switch is rebooted the DLCS information is lost. However, this information is still stored in the Enterprise Manager database. To delete the information from the policy system, you must explicitly delete the configuration parameters using the Enterprise Manager Policy System client.

An alternative is to delete the rebooted switch from the ExtremeWare Enterprise Manager database using the Delete Device function in the Inventory Manager. Then re-add the switch using the Inventory Manager Add Device function.

- DLCS is not currently supported on hosts with multiple NIC cards.

ISQ IMPROVEMENTS

Intra-Subnet QoS has been improved to also allow the application of IP QoS for traffic on a Layer 2 switch that is destined outside the served subnet. If your switch is running in L2 mode, and you want to snoop Layer 4 (NetBIOS) packets, you can do so using ISQ.

To configure this capability, you will need the MAC address of the next-hop router (or the MAC address of the WINS server, if the server is on the same subnet) and a list of the IP addresses of the WINS servers. The IP packets to this MAC address and the specified IP addresses are then snooped.

After DLCS has been enabled, the following commands should be used for this configuration:

- Create a list of WINS servers whose packets should be snooped:

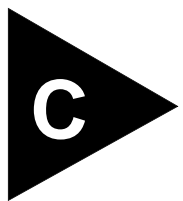
```
create isq-server <name>
```

- Add the WINS server IP addresses to this list:

```
config isq-server <name> add ipaddress <WINS-server-ipaddress1>
config isq-server <name> add ipaddress <WINS-server-ipaddress2>
...
```

- Configure the MAC address of the next hop router:

```
config isq-server <name> add mac <mac-address-of-next-hop> vlan <vlan-name>
```



Database Utilities

This chapter describes:

- The DBVALID command-line database validation utility.
- The DBBACKUP command-line database backup utility

OVERVIEW

Sybase database validation and backup utilities are shipped with the ExtremeWare Enterprise Manager software.

The Validation utility validates all indexes and keys on some or all of the tables in the database. The Validation utility scans the entire table and looks up each record in every index and key defined on the table.

This utility can be used in combination with regular backups to give you confidence in the security of the data in your database.

The Backup utility makes a backup copy of all data in the database, except for user names and passwords, which are kept in separate files. Backing up your database regularly will ensure that you will not need to re-enter all the switch, VLAN, QoS, and VC stack information in the event that the database is corrupted or destroyed.

Both database utilities are found in the `<install_dir>\database` directory. `<install_dir>` is the directory where you installed the ExtremeWare Enterprise Manager software. Substitute the name of the actual directory for `<install_dir>` when you run these commands.

THE VALIDATION UTILITY

The Validation utility validates all indexes and keys on some or all of the tables in the database. Access the Validation utility from the MSDOS or Solaris command line using the **dbvalid** command. This convention also allows incorporation into batch or command files.

USING THE DBVALID COMMAND-LINE UTILITY

To validate the ExtremeWare Enterprise Manager database running under Windows NT, use the command:

```
<install_dir>\database\dbvalid -c "uid=dba;pwd=sql;dbf=<install_dir>\basecamp.db"
```

Under Solaris, use the command:

```
<install_dir>/database/dbvalid -c "uid=dba;pwd=sql;dbf=<install_dir>/basecamp.db"
```

This example assumes a database user ID of **dba**, with password **sql**. These are the defaults used when the database server is installed through the ExtremeWare Enterprise Manager installation process. If you have changed your database user ID and password, substitute your actual user ID and password in the command.

<install_dir> is the directory where the Enterprise Manager software is installed. Substitute the actual directory name in the command.

This operation should report no errors. If there are errors, the system should be stopped and a backup database copied into place. See "Installing a Backup Database" later in this appendix. If there are no backups, the Enterprise Manager software will need to be re-installed.

Syntax: **dbvalid** [*switches*]

Table C-1: dbvalid Command Switches

Switch	Description
-c "keyword=value; ..."	Supply database connection parameters

DATABASE CONNECTION PARAMETERS

These are the parameters for the `-c` command-line switch. If the connection parameters are not specified, connection parameters from the `SQLCONNECT` environment variable are used, if set.

Table C-2: Database Connection Parameters for `dbvalid` Utility

<code>uid=<user name></code>	The user name used to login to the database. Default is dba . The user ID must have DBA authority.
<code>pwd=<password></code>	The password used to login to the database. Default is sql .
<code>dbf=<database_file></code>	The name of the file that stores the data. This is the file to be validated.

The connection parameters are separated by semi-colons, and the entire set must be quoted. For example, under Windows NT the following validates the ExtremeWare Enterprise Manager, connecting as user ID **dba** with password **sql**:

```
<install_dir>\database\dbvalid -c "uid=dba;pwd=sql;dbf=<install_dir>\basecamp.db"
```

THE BACKUP UTILITY

The Backup utility makes a backup copy of all data in the database, except for user names and passwords. Access the Backup utility from the MSDOS or Solaris command line using the **dbbackup** command. This convention also allows incorporation into batch or command files.

THE DBBACKUP COMMAND-LINE UTILITY

To back up the ExtremeWare Enterprise Manager database running under Windows NT, use the command:

```
<install_dir>\database\dbbackup -c  
"uid=dba;pwd=sql;dbf=<install_dir>\basecamp.db" <backup_dir>
```

Under Solaris, use the command:

```
<install_dir>/database/dbbackup -c  
"uid=dba;pwd=sql;dbf=<install_dir>/basecamp.db" <backup_dir>
```

This example assumes a database user ID of `dba`, with password `sql`. These are the defaults used when the database server is installed through the ExtremeWare Enterprise Manager installation process. If you have changed your database user ID and password, substitute your actual user ID and password in the command.

`<install_dir>` is the directory where the Enterprise manager software is installed. Substitute the actual directory name in the command.

`<backup_dir>` is the directory where the backup copy of the database should be stored. Substitute an actual directory name in the command.

This command generates a backup of the database in the specified backup directory. The backup consists of two files, `basecamp.db` and `basecamp.log`. All database files are backed up. These files should be saved so they can be used to replace the original files in the event of a problem.

Syntax: **dbbackup** *[switches] directory*

Table C-3: dbbackup Command Switches

Switch	Description
-c "keyword=value; ..."	Supply database connection parameters
-y	Replace files without confirmation

DATABASE CONNECTION PARAMETERS

These are the parameters for the `-c` command-line switch. If the connection parameters are not specified, connection parameters from the `SQLCONNECT` environment variable are used, if set.

Table C-4: Database Connection Parameters for dbbackup Utility

<code>uid=<user name></code>	The user name used to login to the database. Default is dba . The user ID must have DBA authority.
<code>pwd=<password></code>	The password used to login to the database. Default is sql .
<code>dbf=<database_file></code>	The name of the file that stores the data. This is the file to be backed up.

The connection parameters are separated by semi-colons, and the entire set must be quoted. For example, under Windows NT the following backs up the ExtremeWare Enterprise Manager database `basecamp.db`, connecting as user ID **dba** with password **sql**:

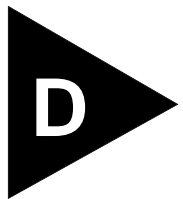
```
<install_dir>\database\dbbackup -c  
"uid=dba;pwd=sql;dbf=<install_dir>\basecamp.db" c:\tmp
```

INSTALLING A BACKUP DATABASE

The backup database is named `basecamp.db`, and is kept in the directory you specified when you ran the **dbbackup** command (`c:\tmp` in the example).

To replace a damaged database with the backup copy, follow these steps:

- 1 Shut down the ExtremeWare Enterprise Manager following the instructions in Chapter 3, in the section “Shutting Down the Enterprise Manager Server Components” for your operating system environment.
- 2 Move or delete the old copy of `basecamp.db` found in the Enterprise Manager installation directory.
- 3 Copy the backup copy of `basecamp.db` to the Enterprise Manager installation directory.
- 4 Restart the Enterprise Manager following the instructions in Chapter 3 for your operating system environment.



ExtremeWare Enterprise Manager Properties Files

This chapter describes several properties files used by ExtremeWare Enterprise Manager:

- `extreme.properties` — ExtremeWare Enterprise Manager configuration parameters.
- `ciscoipports.properties` — Cisco's mapping of names to well-known ports.

These files are both found in the `extreme` subdirectory of the installation directory (by default `eem2_0\extreme`).

THE `extreme.properties` FILE

This file contains default values for a number of ExtremeWare Enterprise Manager configuration parameters, including the SNMP polling interval, the SNMP request time-out, the number of SNMP request retries, and several timeout values. This file is found in the `<install_dir\extreme>` directory. The defaults and value restrictions are as indicated in the file, listed below.

```
#This file has user configurable parameters for SNMP operations.
```

```
#Polling interval in seconds to refresh status of each switch
#Default=300, Minimum=5, Maximum=3600 (1 hour)
Snmp.PollInterval=300
```

```
# Number of seconds after which an SNMP request should first time out.
# This is followed by an exponential backoff
# Default=2, Minimum=1, Maximum=10 seconds
```

```

Snmp.TimeoutPeriod=2

# Number of retries before timing out.
# Default=1, Minimum=0, Maximum=5
Snmp.NumberOfRetries=1

# Enables ExtremeView to save switch user names and passwords in the database
# automatically.
# Default = true, Disable with false
SaveSwitchPassword=true

# Timeout period in milliseconds after EEM terminates after which the user is
# required to relogin
# Default = 60000 milliseconds (10 Min), Disable with -1
Session.TimeoutPeriod=60000

# Timeout period in milliseconds to be used when performing DNS lookups
# for hosts found through DLCS or when importing through Domain Controller
# Default: 1000
Dns.LookupTimeoutPeriod=1000

```

THE ciscoipports.properties FILE

This file documents the mapping between well-known ports and the names that Cisco devices will substitute when they encounter these ports. The ExtremeWare Enterprise Manager policy system uses this file to determine how to change the names back to port numbers. You can edit this file to add any mappings that may be missing. This file is found in the `<install_dir>\extreme>` directory.

```

bgp          = 179
biff         = 512
bootpc      = 68
bootps      = 67
chargen     = 19
cmd         = 514
daytime     = 13
discard     = 9
dnsix       = 195

```

domain	= 53
echo	= 7
exec	= 512
finger	= 79
ftp	= 21
ftp-data	= 20
gopher	= 70
hostname	= 101
ident	= 113
irc	= 194
isakmp	= 500
klogin	= 543
kshell	= 544
login	= 513
lpd	= 515
mobile-ip	= 434
nameserver	= 42
netbios-dgm	= 138
netbios-ns	= 137
netbios-ss	= 139
nntp	= 119
ntp	= 123
pim-auto-rp	= 496
pop2	= 109
pop3	= 110
rip	= 520
smtp	= 25
snmp	= 161
snmptrap	= 162
sunrpc	= 111
syslog	= 514
tacacs	= 49
talk	= 517
telnet	= 23
tftp	= 69
time	= 37
uucp	= 540
who	= 513
whois	= 43
www	= 80
xdmcp	= 177

Troubleshooting

This appendix describes:

- Resolving problems you may encounter using the ExtremeWare Enterprise Manager Server.
- Resolving problems you may encounter using the ExtremeWare Enterprise Manager client application.

EXTREMEWARE ENTERPRISE MANAGER SERVER ISSUES

INSTALLATION

Problem: The Windows NT installation wizard automatically imported the database from the most recent previous version of ExtremeWare Enterprise Manager, when I wanted to import from an older version (e.g. 1.0 instead of 1.1).

Uninstall all versions of ExtremeWare Enterprise Manager except the one from which you want to import the database. Then install the new version. See the instructions in Chapter 2 for information on un-installing ExtremeWare Enterprise Manager.

Problem: Under Windows NT, cannot install ExtremeWare Enterprise Manager on system where HP OpenView is running.

The InstallShield wizard does not run when HP OpenView services are running. You must stop the HPOV services, do the ExtremeWare Enterprise Manager installation, and then restart the HPOV services.

SNMP

Problem: Cannot talk to a specific switch.

Verify that the switch is running ExtremeWare software version 2.0 or greater.

Ping the switch's IP-address to verify availability of a route. Use the `ping` command from a MS-DOS or Solaris command shell.

Verify that the read and write community strings used in the ExtremeWare Enterprise Manager match those configured on the switch.

Problem: ExtremeWare CLI or ExtremeWare Vista changes are not reflected in ExtremeWare Enterprise Manager.

Verify that the switch is running ExtremeWare software version 2.0 or greater.

From the Inventory Manager, click **Sync** to update the information from the switch . This refreshes the switch specific data, validates the SmartTrap rules, and ensures that the Enterprise Manager server is added as a trap receiver (Extreme switches only).

If the problem persists, verify that the ExtremeWare Enterprise Manager workstation has been added in the list of trap destinations on the given switch:

- 1 Telnet to the switch.
- 2 Login to the switch.
- 3 Type `show management` to verify that the system running the Enterprise Manager is a trap receiver.

An Extreme switch can support up to a maximum of 6 trap destinations in ExtremeWare 2.0, and up to 15 trap destinations with ExtremeWare 4.1 or greater. If ExtremeWare Enterprise Manager is not specified as a trap destination, then no SmartTraps are sent, and the data is not refreshed. If you need to remove a trap receiver, use the command:

```
config snmp delete trapreceiver <ipaddress>
```

For details, see the [ExtremeWare 4.0 Software User Guide](#) or the [ExtremeWare Command Reference](#) manual.

Problem: Need to change polling interval, SNMP request time-out, or number of SNMP request retries.

To change the default values for the SNMP polling interval, the SNMP request time-out, or the number of SNMP request retries, edit the file `extreme.properties`, found in the `<install_dir>\extreme` directory. The defaults and value restrictions are as indicated in the file, as shown. The full properties file is listed in Appendix D.

```
#Polling interval in seconds to refresh status of each switch
#Default=300, Minimum=5, Maximum=3600 (1 hour)
Snmp.PollInterval=300

# Number of seconds after which an SNMP request should first time out.
# This is followed by an exponential backoff
# Default=2, Minimum=1, Maximum=10 seconds
Snmp.TimeoutPeriod=2

# Number of retries before timing out.
# Default=1, Minimum=0, Maximum=5
Snmp.NumberOfRetries=1
```

VLANs

Problem: Can only access one of the IP addresses on a VLAN configured with IP multi-netting.

ExtremeWare Enterprise Manager does not currently support IP multi-netting.

Problem: Configuration fails when attempting to configure a VLAN with a modified protocol definition.

ExtremeWare Enterprise Manager does not have a mechanism to modify protocols. When a VLAN is configured through ExtremeWare Enterprise Manager to use a protocol that does not exist on the switch, the protocol is first created on the switch. However if a protocol with the same name, but a different definition already exists on the switch, the operation will fail.

Problem: An untagged port has disappeared from its VLAN.

Check to see if the port has been added as an untagged port to a different VLAN. In ExtremeWare Enterprise Manager, adding an untagged port to a VLAN automatically removes the port from its previous VLAN if the port was an untagged port, and the new and old VLANs used the same protocol. This is different behavior from the ExtremeWare CLI, where you have to first delete the port from the old VLAN before you can add it to the new VLAN.

EXTREMEWARE ENTERPRISE MANAGER CLIENT

CLIENT INITIALIZATION

Problem: Browser is unable to connect to the ExtremeWare Enterprise Manager server.

Verify that the ExtremeWare Enterprise Manager Server process is running.

Verify that the server is running on the specified port. Check the file `<installdir>\webserver\properties\server\javaWebServer\webPageService\endpoints.properties`. The entry `endpoint.main.port` contains the port number the server is using.

Problem: Browser does not bring up the Login page.

Verify the version of the browser you are using. See the system requirements in Chapter 2 or refer to the Release Notes shipped with the software.

Problem: Client software loads and allows login, but data is missing or other problems arise.

Clear the browser's cache, exit the browser and restart it. This frequently clears up miscellaneous start-up problems in the client.

For Internet Explorer, clear cache by selecting **Internet Options** under the **View** Menu, then clicking **Delete Files** under the Temporary Internet Files section of the General tab.

VLAN MANAGER

Problem: Multiple VLANs have the same name.

A VLAN is defined by the name, its tag value, and its protocol filter definition. ExtremeWare Enterprise Manager allows multiple VLANs of the same name if one of the other defining characteristics of one VLAN is different from the other.

Problem: Multiple protocols have the same name.

ExtremeWare Enterprise Manager allows multiple protocols of the same name if one of the other defining characteristics of one protocol is different from the other.

Problem: Created a new protocol in VLAN Manager, but the protocol does not appear on any switch.

When a new protocol is created, it is stored in the Enterprise Manager database. The Enterprise Manager only creates the protocol on a switch when the new protocol is used by a VLAN on that switch.

INVENTORY MANAGER

Problem: Discovery hangs if a large number of addresses is specified.

A very large discovery can cause the discovery process to hang because there is insufficient memory available to the browser to process the number of addresses. This is a limitation of the browser.

To recover, restart the browser. Then split your discovery request into multiple requests that involve a smaller number of addresses. Discovery prodisplays a warning if your request involves more than 1500 IP addresses. The actual number of addresses you can successfully poll will depend on the amount of memory available at that time in your browser (browser memory is shared among the various running applets).

Problem: Multiple switches have the same name.

This is because the sysName of those switches is the same. Typically, Extreme Networks switches are shipped with the names "Summit1," "Summit2," "Summit4," or "Summit48," depending on the type of switch. You should change these names to unique names using the ExtremeWare CLI or ExtremeWare Vista.

POLICY SYSTEM CLIENT

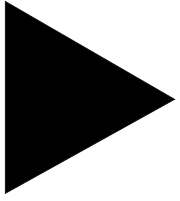
Problem: Cannot Import users from NT Domain Controller

The ExtremeWare Enterprise Manager Server must be running with permissions that enable it to get user information from a Domain Controller. To verify and change permissions for the Web Server, do the following:

- 1 From the **Start** menu, highlight **Settings**, pull right, and click on the **Control Panel**. This displays the Control Panel folder.
- 2 Double-click on **Services** to display the Services Properties window.
- 3 Highlight “EEM 2.0 Web Server” in the list of services, and click the **Startup...** button.
- 4 In the “Log On As:” section of the pop up window, enter the account name and password for a user that has the appropriate permissions to access the Domain Controller.
- 5 Stop and Restart the Web Server service to have the new user log on take effect.

Problem: The “Policy Configured” field in the Policy View Status page shows the message “Error: Too many rules”

This message means you need to reduce the number of endpoints that your policy specifies.



Index

Numerics

802.1Q tag 7-2, 7-7

A

About button 3-9

access levels 1-5, 4-1

Add button

 in Inventory Manager 5-5

 in VLAN Manager 7-6

adding

 devices 5-13

 end station groups as policy objects 8-50

 end stations as policy objects 8-48

 protocol filters 7-14

 user accounts 4-6

 user groups as policy objects 8-47

 users as policy objects 8-44

 VLANs 7-6

address ranges

 in discovery 5-9

Admin button 3-9

Admin Port 2-4

Administration page 4-3

Administrator

 adding users 4-6

 changing password 4-4

 deleting a user account 4-7

 ExtremeWare 4-2

 modifying users 4-6

Administrator access level 1-5

 Enterprise Manager 4-2

Administrator password

 default 4-3

All Device Groups page 5-4

Application

 as policy object 8-7

Application Server policy 8-2

Application Server policy definition tab 8-24

architecture

 Enterprise Manager software 1-6

Auto Configure button (Policy) 8-14

B

buttons 3-13

 About 3-9

 Add (Inventory Manager) 5-5

 Add (VLAN Manager) 7-6

 Admin 3-9

 Auto Configure (Policy) 8-14

 Configure (Inventory Manager) 5-5

 Configure (VC Stack Manager) 9-5

 Create (VC Stack Manager) 9-5, 9-10

 Create Policy 8-14, 8-15

 Delete (Inventory Manager) 5-5

 Delete (Policy) 8-14

 Delete (VC Stack Manager) 9-5, 9-11

 Delete (VLAN Manager) 7-9

 Discover 5-5

 Edit (VC Stack Manager) 9-5, 9-12

 EView 3-10

 Find IP/MAC 3-10

 Identify (VC Stack Manager) 9-5

 Inventory 3-9

 Logoff 3-10

 Modify (Inventory Manager) 5-5

 New (Policy) 8-14

 Policy 3-10, 8-13

- RT Stats 3-10
- Sync (Inventory Manager) 5-5, 5-25
- Up (Policy) 8-14
- VC 3-9, 9-3
- VLAN 3-9

C

- changing password
 - for Administrator 4-4
 - user 4-8
- Cisco device requirements 1-8
- Cisco device support
 - in Policy System 8-9
- client
 - installation 2-14
 - launching from HP OpenView A-9
 - starting 3-5
 - starting for first time 4-3
- client browser requirements 1-10
- Client/Server policy 8-3
- Client/Server policy definition tab 8-27
- columns
 - sorting 3-13
- Command Line Interface 1-3
- community string
 - in Discovery 5-10
- Component Tree 3-11
 - moving the boundary 3-13
- Configure button 5-5
- Configure button (VC Stack Manager) 9-5
- conventions
 - text, About This Guide xviii
- Create button (VC Stack Manager) 9-5, 9-10
- create policy
 - New menu 8-20
 - Wizard 8-15
- Create Policy button 8-14, 8-15
- Create Policy Wizard 8-15
- creating
 - VC stack 9-10
 - VLANs 7-6
- Current State block (Policy System) 8-56
- Custom policy 8-5
- Custom policy definition tab 8-32

D

- database backup utility C-3
- database validation utility C-1
- dbbackup utility C-3
- dbvalid utility C-1
- Default device group 5-4
- Definition tab 8-23
 - Application Server policy 8-24
 - Client/Server Policy 8-27
 - Custom policy 8-32

- Source Port policy 8-30
- VLAN policy 8-23
- Delete button 9-11
 - in Inventory Manager 5-5
 - in VC Stack Manager 9-5
 - in VLAN Manager 7-9
- Delete button (Policy) 8-14
- deleting 9-11
 - a switch 5-23
 - a user account 4-7
 - protocol filters 7-13
 - VLANs 7-9
- Device
 - as policy object 8-7
- Device Discovery set up window 5-9
- Device Group
 - as policy object 8-7
- device groups 5-2
 - default 5-4
- device status
 - Inventory Manager 5-6
- dialog boxes 3-14
- Discover button 5-5
- Discovery 1-4, 5-2, 5-8
 - address range 5-9
 - community string 5-10
 - subnet mask 5-10
- displaying a VC stack 9-5
- DLCS
 - automatic updates 8-46, 8-50
 - lookup or end station 8-49
- Dynamic Link Context System (DLCS) 1-4

E

- Edit button (VC Stack Manager) 9-5, 9-12
- editing a VC stack 9-12
- end station group
 - as policy object 8-7
 - Policy System 8-50
- end stations 8-14
 - as policy object 8-7
 - importing 8-57
 - Policy System 8-48
- End Stations (Policy System) 8-14
- Enterprise Manager
 - architecture 1-6
 - client 2-14
 - components 1-6
 - logging in 3-8
 - server components 2-2, 3-2
 - server requirements 1-9
- evaluation copy 2-3
 - updating to full license 2-5, 2-12
- Event Log (Policy System) 8-14
- EView button 3-10
- Extreme switch requirements 1-8

ExtremeView 1-2
Telnet 1-3
ExtremeWare Vista
launching from HP OpenView A-11

F

Find IP/MAC button 3-10

H

heartbeat check 1-8
HP OpenView
launching client from A-9
launching ExtremeWare Vista from A-11
HP OpenView integration 2-5
(Solaris) A-4
uninstalling A-9
(Windows NT) A-2
uninstalling A-4
requirements 1-10
HTTP port 2-4

I

Identify button (VC Stack Manager) 9-5
Identifying Virtual Chassis stack topologies
VC Stack Manager
identifying stack topologies 9-2
Implementation types 8-8
implementation types
IP QoS 8-8
Source Port QoS 8-8
VLAN QoS 8-8
Import (Policy System) 8-14
Import (Policy) 8-57
in VC Stack Manager 9-11
installing the client 2-14
installing the server
as a service (Windows NT) 2-4
under Solaris 2-7
under Windows NT 2-2
integration with HP OpenView
(Solaris) A-4
(Windows NT) A-2
Inventory button 3-9
Inventory Manager 1-4
adding devices 5-13
Discovery 5-8
Inventory Manager page 5-3
IP QoS implementation type 8-8
IP/MAC Address Finder 1-5

L

license key 2-3

logging in 3-8
Login page 3-8, 4-3
Logoff button 3-10

M

Managed Devices (Policy System) 8-14
Manager access level 1-5, 4-1
menu
New (Policy System) 8-14, 8-15
Modify button
in Inventory Manager 5-5
in VLAN Manager 7-10
modifying
end station groups as policy objects 8-50
end stations as policy objects 8-48
network policies 8-21
network QoS treatment 8-42
switch contact information 5-18
user accounts 4-6
user groups as policy objects 8-47
users as policy objects 8-44
VLANs 7-10
Monitor access level 1-5, 4-1

N

Navigation Toolbar 3-9
Network Policy (Policy System) 8-13
Network QoS Policy view 8-21
New button (Policy) 8-14
New menu 8-15
Policy 8-20

O

orphan Summits 9-5
displaying 9-8
orphan VCs 9-4
displaying 9-7
Overlaps tab (Policy) 8-37

P

passwords
changing for Administrator 4-4
default 4-3
users changing 4-8
Policy
definition 8-5
Policy button 3-10, 8-13
Policy Implementation types 8-8
policy object 8-7
Policy overlaps 8-37
Policy precedence 8-37, 8-38
Policy Scoping 8-8, 8-35

- Policy System 1-4, 8-1
 - adding end station groups 8-50
 - adding end stations 8-48
 - adding users 8-44
 - adding user groups 8-47
 - Auto Configure 8-14
 - Cisco devices 8-9
 - Configuration 8-14
 - Create Policy button 8-14
 - Delete button 8-14
 - End Stations 8-14
 - Event Log 8-14
 - Import 8-14, 8-57
 - Managed Devices 8-14
 - modifying end station groups 8-50
 - modifying end stations 8-48
 - modifying user groups 8-47
 - modifying users 8-44
 - Network Policy 8-13
 - New button/menu 8-14
 - Up button 8-14
 - Users 8-13
 - using 8-13
 - Xedia devices 8-11
- Policy Type
 - in Create Policy Wizard 8-15
 - specifying 8-15
- policy types 8-2
 - Application Server policy 8-2
 - Client/Server policy 8-3
 - Custom policy 8-5
 - Source Port policy 8-3
 - VLAN policy 8-4
- Policy-based management 8-1
- Policy-Based Quality of Service 1-4
- polling 5-3
- Port Group
 - as policy object 8-7
- port groups 5-2
- ports
 - removing from a VLAN 7-8
 - removing from VLAN 7-11
- Precedence tab (Policy) 8-38
- precedence type 8-37
- protocol filters 7-2, 7-7
 - adding 7-14
 - changing in VLAN 7-10
 - deleting 7-13

Q

- QoS
 - default QoS profiles 8-43
- QoS Results tab(Policy) 8-41

R

- RADIUS server 4-2
 - administering 4-9
 - changing port 4-10
 - changing shared secret 4-10
 - disabling 4-10
 - enabling 4-10
- Ready/Busy indicator (Policy System) 8-14
- Real Time Statistics 1-5, 10-1
- related publications, About This Guide xviii
- Release Notes xvii
- Remote Authentication Dial In User Service (RADIUS) 1-6
- resizing
 - columns in status display 3-13
 - Component Tree 3-13
- restarting the server
 - under windows NT 3-3
- RT Stats button 3-10
- running the client 3-5

S

- scope
 - treatment 8-44
- Scope tab (Policy) 8-35
- Scope, policy 8-35
- scope, policy 8-8
- server installation
 - under Solaris 2-7
 - under Windows NT 2-2
- server system requirements
 - Solaris 1-9
 - Windows NT 1-9
- SmartTraps 1-7, 5-3
- SNMP 5-2
- software architecture 1-6
- software components 1-6
- Solaris
 - HP OpenView integration A-4
 - patches for 2.6 2-7
 - patches for Solaris 7 2-7
 - server installation 2-7
 - starting the server 3-4
 - stopping the server 3-4
 - uninstalling HP OpenView integration A-9
 - uninstalling the server 2-13
- sorting columns 3-13
- Source Port policy 8-3
- Source Port policy definition tab 8-30
- Source Port QoS implementation type 8-8
- starting the server
 - under Solaris 3-4
 - under Windows NT 3-2
- Status tab (Policy) 8-34
- Status/Detail Information panel 3-11

- stopping the server
 - under Solaris 3-4
 - under Windows NT 3-2

Subnet

- as policy object 8-7

subnet mask

- in Discovery 5-10

Summit switch

- configuring ports in VC Stack Manager 9-2
- deleting 5-23
- displaying orphan Summits 9-8
- modifying contact information 5-18
- updating status 5-25

switch polling 5-3

- Sync button 5-3, 5-5, 5-25

T

- tagged ports 7-8

- Telnet 1-3

- terminology, About This Guide xviii

- Third-Party Device Requirements 1-8

third-party devices

- support in Policy System 8-9

Treatment

- as policy object 8-7
- modifying 8-42
- scope 8-44
- viewing 8-42

U

- uninstalling the HP Openview integration (Solaris) A-9

- (Windows NT) A-4

uninstalling the server

- under Solaris 2-13
- under Windows NT 2-6

- untagged ports 7-8

- Up button (Policy) 8-14

- updating switch information 5-25

User

- as policy object 8-7
- ExtremeWare 4-2

- User Administration page 4-3

User Group

- as policy object 8-7

user groups

- Policy System 8-47

Users

- (Policy System) 8-13
- Policy System 8-44

users

- importing in Policy System 8-57

- users, adding 4-6

- users, modifying 4-6

utilities

- database backup C-3

- database validation C-1

V

- VC button 3-9, 9-3

- VC Stack 9-11

- VC Stack Manager 1-3, 9-1

- configuring switch ports 9-2

- creating a VC stack 9-10

- deleting a VC stack 9-11

- displaying a VC stack 9-5

- displaying orphan Summits 9-8

- displaying orphan VCs 9-7

- editing a VC stack 9-12

- orphan Summits 9-5

- orphan VCs 9-4

- VC Stack Manager page 9-4

View Policy

- Definition tab 8-23

viewing

- network policies 8-21

- network QoS treatments 8-42

- Virtual Chassis 1-3, 9-1

- Virtual Chassis stack 9-1

- Virtual Chassis Stack Manager. *See* VC Stack Manager

- Virtual LANs. *See* VLANs

- VLAN button 3-9

- VLAN Manager 1-3

- VLAN Manager page 7-3

- VLAN policy 8-4

- VLAN policy definition tab 8-23

- VLAN QoS implementation type 8-8

- VLANs 1-3

- adding 7-6

- adding protocol filters 7-14

- adding tagged ports 7-8

- adding untagged ports 7-8

- as policy object 8-7

- criteria 7-2

- deleting 7-9

- deleting protocol filters 7-13

- displaying 7-3

- modifying 7-10

- remove a port 7-8

- removing ports 7-11

W

wildcards

- in Discovery addresses 5-9

Windows NT

- HP OpenView integration A-2

- restarting the server 3-3

- server installation 2-2

starting the server 3-2
stopping the server 3-2
uninstalling HP OpenView integration A-4
uninstalling the server 2-6

X

Xedia device requirements 1-8
Xedia device support
in Policy System 8-11